

DEPARTMENT OF HOMELAND SECURITY APPROPRIATIONS FOR FISCAL YEAR 2012

WEDNESDAY, MARCH 2, 2011

U.S. SENATE,
SUBCOMMITTEE OF THE COMMITTEE ON APPROPRIATIONS,
Washington, DC.

The subcommittee met at 10:05 a.m., in room SD-138, Dirksen Senate Office Building, Hon. Mary L. Landrieu (chairman) presiding.

Present: Senators Landrieu, Lautenberg, Coats, Cochran, Murkowski, and Moran.

DEPARTMENT OF HOMELAND SECURITY

STATEMENT OF HON. JANET NAPOLITANO, SECRETARY

OPENING STATEMENT OF SENATOR MARY L. LANDRIEU

Senator LANDRIEU. Good morning. I would like to call our subcommittee to order for the purpose of considering the Department's budget for 2012.

Let me first welcome our new ranking member, Senator Coats. I am pleased to work with Senator Coats in the next 2 years and really appreciate his leadership in this area.

Welcome, Madam Secretary. We are happy to have you present your budget this morning. You lead a Department of 221,000 men and women who are on the front lines every day protecting our Nation and our citizens. And we commend those employees for their dedication and their hard work. They are in our airports, our ports, along our borders, considering the intelligence coming in all over our country, we appreciate their work and we appreciate your leadership.

My goal is to produce a bipartisan, fiscally responsible Homeland Security bill for fiscal year 2012 that provides this Department with the resources it needs to prepare for, respond to, and recover from all threats, manmade and natural. I share your commitment to the goals established in the Quadrennial Homeland Security Review: preventing terrorism, securing our borders, enforcing our immigration laws, safeguarding cyberspace, and ensuring resiliency in the face of natural or manmade disasters.

Securing this Nation is not just, as you know, Madam Secretary, a Federal Government responsibility. State and local governments share that responsibility, and frankly, as well as many of our corporations who are doing their part and individual citizens as they are trained to recognize threats that potentially are occurring in

their local communities. This Department must—I believe—serve as leaders and educators in helping our State and local governments and corporations, serving as a model for them, as well as encouraging our private citizens to do their part.

As we approach the 10th anniversary of the 9/11 attacks, the 8th anniversary of the creation of the Department, and the 6th anniversary of the catastrophic levee failures which caused horrific destruction in and around the city of New Orleans, the hurricanes of Katrina and Rita along the gulf coast, we must not let our guard down. We must remember the lessons of those horrific events and, even without the imminent threat right before us, not fail to remember what we learned on those terrible occasions. We must have the fortitude and the discipline and the tenacity I think, Senator Coats and others, to continue to fund adequately this effort and not become lax or distracted.

In the State of the Union Address, the President said that al Qaeda and its affiliates continue to plan attacks against us. He said, “as extremists try to inspire acts of violence within our borders, we are responding with the strength of our communities and with respect to the rule of law.” Secretary Napolitano, you have stated that the terrorism threat is at the highest level since 9/11. That is a statement that we should pay attention to.

We will be mindful of those statements as we consider the President’s request for this 2012 year. I am supportive of reducing spending where we can, obviously eliminating mediocre programs or duplicative programs. But I do not believe the notion of reducing spending arbitrarily to a 2008 level for this Department makes any sense.

The Coast Guard would have to eliminate 2,400 personnel and its recapitalization program would be terminated. We saw what the Coast Guard did in responding to the BP oil spill. I do not believe a cutback there is smart.

We would have to eliminate the national security cutter, the fast response cutter, and the marine patrol aircraft. The number of customs officers at our ports of entry would be reduced by more than 1,600. The number of Border Patrol agents—Senator McCain has fought very hard, along with others, to secure more personnel at our borders, not less, and I will not support a budget that reduces that number by 3,500.

Reducing funding for the Transportation Security Administration to levels before the Christmas Day bombing attempt would be reckless. We know that there are attempts to take down aircraft in America that are ongoing. We have been successful in preventing it so far. This budget supports our effort to continue to be successful.

We would have 775 fewer scanners at our airports, 4,000 fewer screeners, 330 fewer air cargo inspectors, and 235 fewer canine teams. Under my leadership, we will not go in that direction.

I believe the President has submitted a fiscally responsible budget for this Department. Of course, we will have some issues within the Department. I look forward to working with my ranking member to find a way forward that provides the resources necessary, however, to keep our Nation and our citizens safe.

PREPARED STATEMENT

Following Senator Coats's opening statement, we will hear from you Madam Secretary, because our schedule has changed. I wanted the members to have time for opening statements, but I am going to ask them to submit them for the record because a vote has been called for 11 o'clock.

But let me turn to my ranking member and thank Senator Cochran for joining us this morning.

[The prepared statement follows:]

PREPARED STATEMENT OF SENATOR MARY L. LANDRIEU

Good morning.

Secretary Napolitano, you lead a Department of 221,000 men and women who are on the front lines every day protecting our citizens. We commend those employees for their dedication and their service and we welcome you to this subcommittee hearing today. I also welcome Senator Dan Coats, our new ranking member. I look forward to working with you and hearing from all of our subcommittee members this year.

My goal is to produce a bipartisan, fiscally responsible Homeland Security bill for fiscal year 2012 that provides the Department with the resources it needs to prepare for, respond to, and recover from all threats, both man-made and natural. I share your commitment to the goals established in the Quadrennial Homeland Security Review, preventing terrorism, securing the borders, enforcing our immigration laws, safeguarding cyberspace, and ensuring resilience to disasters.

Securing this Nation is not just about the Federal Government. We must also serve as leaders and educators in helping State and local governments, the private and nonprofit sectors, and our citizens in achieving these goals.

As we approach the 10th anniversary of the 9/11 attacks, the 8th anniversary of the creation of this Department, and the 6th anniversary of Hurricanes Katrina and Rita, we must all learn from history while confronting the evolving threats to this Nation.

In the State of the Union Address, the President said that al Qaeda and its affiliates continue to plan attacks against us. He said, "as extremists try to inspire acts of violence within our borders, we are responding with the strength of our communities, and with respect for the rule of law". Secretary Napolitano, you have stated that the terrorism threat is at its highest level since 9/11.

We will be mindful of those statements as we consider the President's request for fiscal year 2012. While I am supportive of reducing spending, I do not believe the notion of reducing spending to 2008 levels is either appropriate or responsible for the Department of Homeland Security. The Coast Guard would have to eliminate 2,400 personnel and its recapitalization program would be terminated, including the national security cutter, the fast response cutter, and the maritime patrol aircraft. The number of Customs officers at our ports of entry would be reduced by more than 1,600, reducing security and extending wait times. The number of Border Patrol agents would be reduced by more than 3,500, reversing the progress we have made in securing our borders. Reducing funding for the Transportation Security Administration to levels before the Christmas Day bombing attempt would be absurd. We would have 775 fewer scanners at our airports, 4,000 fewer screeners, 330 fewer air cargo inspectors, and 235 fewer canine teams. Under my leadership, we will not go down that road.

I believe the President has submitted a responsible, fiscally prudent budget for the Department of Homeland Security. Of course, we have some issues with the budget which we will discuss today, and I look forward to hearing from the Secretary.

Following Senator Coats' opening statement, each member will be recognized for up to 3 minutes for opening remarks. After the opening remarks, we will hear from Secretary Napolitano. After, we hear from the Secretary, each member will be recognized, based on order of arrival, for up to 5 minutes for questions. I now recognize Senator Coats for any opening remarks he may wish to make.

STATEMENT OF SENATOR DANIEL COATS

Senator COATS. Madam Chairman, thank you. I am pleased to join you on this subcommittee, my first venture here. So I will

probably have more questions than answers, but I look forward to the testimony.

Secretary Napolitano, thank you for being here this morning and reaching out yesterday with a courtesy call for me and being willing to sit down and talk through difficult, challenging issues at a difficult, challenging time. So I appreciate that very much.

I never thought I would be sitting in a superior position to Senator Cochran on any committee anywhere, including lunch. But it is a pleasure to be with you, Thad, and I appreciate your leadership over the years of this subcommittee and ranking membership is duly noted.

Madam Secretary, I do not think any of us question that we are in difficult fiscal times. Also no one questions whether or not we have security threats that we need to address and need to protect the American people from incursions and unwanted terrorist activity and to do everything we can to provide for homeland security. So there comes the challenge for all of us.

The current budget that the President has announced is an increase over previous years. As you know, the Congress is looking for ways to try to do more with less. The question I think comes in terms of how we can provide effective service and fulfill our obligations in providing for the security of our country, at the same time trying to do it in a more efficient way. We are not asking for no Government here. We are asking for more efficient Government, and working together, I think, to try to achieve that should be one of our goals.

As I look at your budget, a couple of things come to mind, and I just might mention those and we can discuss them during the hearing and afterwards.

The budget indicates—I think assumes—that there will be an increase in aviation passenger security fees and that those fees will start rolling in in the third quarter of fiscal year 2012. Yet, none of that is assured yet, and I am told that that is a mark of nearly \$590 million in additional collections. And so I would like to pursue that question with you.

Second, the budget continues to request operations for disaster relief based on historical obligations for noncatastrophic events and assumes that large catastrophic events are rare and should be funded strictly by supplemental emergency appropriations. As you know, the reality is that those large catastrophic events result in year after year after year of follow-up funding, and whether that should be done by emergency supplemental or budgeted is, I think, a fundamental question that we have to address. My understanding is that for fiscal year 2011, the amount necessary to provide for continuing work post-Katrina, post other catastrophic occurrences is \$1.6 billion, an amount that is not put into the President's budget. And so when you add all this up, I think it totals around \$3 billion not included in the 2012 request. How we are going to reconcile that, I think, is going to be a challenge for us all.

And of course, those assumptions often come in low. We have seen occurrences of more and more violent storms and catastrophic events, whether it is flooding, wildfires, hurricanes, or other disasters.

There are a couple of other areas that I would like to talk about, but we can wait until question time. Again, I thank you for being here and look forward to a year of good, solid work in terms of trying to do more with less funds, but do it more efficiently. Every family in America, every business in America, almost every State in the Union has had to face up to this challenge, and the Federal Government is going to need to do so also.

Thank you.

Senator LANDRIEU. Thank you, Senator, for those remarks.

I want to acknowledge Senator Lautenberg who has joined us. He chaired this subcommittee in the interim after the death of Chairman Byrd, and Senator, thank you for your leadership.

DISASTER RELIEF FUND

We are going to go right into questions in the order of appearance. Let me begin following up on what Senator Coats said about the disaster relief fund, Madam Secretary, which is particularly of interest to gulf coast leaders. But frankly, with the catastrophes in Rhode Island, the flooding in Tennessee, and fires and tornadoes in other parts of the country, there are many members that are very concerned.

For fiscal year 2011, the current year we are in, we are facing a \$1.6 billion gap in the disaster relief fund. If the President does not request and the Congress does not approve supplemental funding, that account under our calculations will literally run out of money in June, only a few months from now, just as we are entering hurricane season.

For fiscal year 2012, the problem is even worse because we are facing a \$3 billion gap based on known costs. These are not projections or speculations. These are known costs of past disasters.

In fiscal year 2010, there was a similar shortfall. FEMA had to stop providing assistance for rebuilding and recovery projects. Many of those were in my home State. Some of them were in Senator Cochran's home State of Mississippi, but they were all over the country. Unfortunately, this problem looks like it is repeating itself, and I would like to head it off, if we can, at the pass.

During the last hearing before the authorizing committee, you said it is "really nonnegotiable" when asked about the looming crisis. You said we have to pay for these disasters. It is our responsibility.

Do you believe that the President is going to send up a supplemental to request this funding, and if so, when? Because if we have to cut \$1.6 billion out of the base Homeland Security budget, that will cut the Coast Guard, that will cut FEMA, that will cut grants to State and local responders, and basically we will be cutting current disaster response teams to pay for past disasters. To me that does not make any sense. Do you think the President will send up a supplemental and would you support it?

Secretary NAPOLITANO. Well, thank you, Senator, and thank you for this hearing. I am pleased to be here before you, Ranking Member Coats, other members of the subcommittee.

I do have an opening statement and I will just simply ask that that be inserted.

Senator LANDRIEU. Please go right ahead with your opening statement.

Secretary NAPOLITANO. Well, I am happy to go right to questions, if you want to do that.

Senator LANDRIEU. No, no, no. You go right to your opening statement. I am very sorry. And then you can take that question.

Secretary NAPOLITANO. All right.

Senator COATS. Maybe it will be happier.

Senator LANDRIEU. Yes. Maybe it will be easier than my question.

Senator LANDRIEU. Go right ahead.

Senator COATS. Whatever works best.

Secretary NAPOLITANO. Well, why don't I answer the question and then I will give the opening statement?

Senator LANDRIEU. Thank you.

Secretary NAPOLITANO. You have identified one of the issues that we will have to work together on and we look forward to working with the subcommittee on.

One of the things that the numbers do not reflect yet is our effort to deobligate funds that have been set aside to pay for past disasters that no longer are necessary. In other words, we have been able to go backwards and say, well, we set aside this amount and in fact we did not need that amount of money. So in fiscal year 2010, for example, we restored \$2 billion to the DRF by process of deobligation. That is what it is called. And so we look forward to continuing that strategy as we move forward to refill the DRF with deobligated funds.

Now, will that be enough to cover expenses for fiscal year 2011 and fiscal year 2012? Probably not without a supplemental of some sort. So we anticipate that the administration will submit a supplemental for the DRF. This has been the historical practice under Republican and Democratic administrations. I think the reason the practice started was because of the difficulty of predicting ultimately what the DRF will be required to cover. So the administration has carried forward with that historical practice, but nonetheless, I think it is fair to say, Madam Chair, that a supplemental will be necessary.

Senator LANDRIEU. Thank you and please go on with your opening statement.

SUMMARY STATEMENT OF JANET NAPOLITANO

Secretary NAPOLITANO. Well, let me begin again by thanking you for the opportunity to discuss the President's fiscal year 2012 budget for the Department of Homeland Security.

I think it is fair to say that the demands on DHS have never been greater. This is especially true as we remember those at the Department who have given their lives in service of the mission of securing our country, including just in the past weeks and months, Border Patrol Agent Brian Terry and ICE Special Agent Jaime Zapata.

Now, Mexico is leading the investigation into the death of Agent Zapata. We are supporting them through a joint DOJ/DHS task force that the Attorney General and I announced 2 weeks ago. Recently, Mexican authorities have apprehended some of the alleged

killers of Agent Zapata, and we are conducting a number of operations in the United States related to the drug cartels that plague that country.

I can speak for the entire administration when I say we are not only saddened by the loss of an agent, we are outraged by this act of violence against an officer of the United States. And make no mistake, justice will be brought to all of those involved. We owe nothing less to the memory of our agent, Agent Zapata, and to those who are still on the job in Mexico.

But the loss of these great agents is a stark reminder of the sacrifices made by the men and women of DHS every day. It also strengthens our resolve to continue to do everything in our power to protect against, mitigate, and respond to threats and to make our Nation more resilient for years to come.

Today's threat picture features adversaries who evolve quickly and are determined to strike us here at home—from the aviation system and the global supply chain to surface transportation, critical infrastructure, and our cyber networks.

We are leading the administration's unprecedented effort to secure our Southwest Border, coupled with a smart and effective approach to enforcing immigration laws in the interior of our country. And we continue to prepare for, respond to, and recover from disasters of all types.

President Obama's fiscal year 2012 budget for the Department allows us to continue to meet these evolving threats and challenges by prioritizing our essential operational requirements while reflecting an unprecedented commitment to fiscal discipline that maximizes the effectiveness of every security dollar that we receive.

Reflecting the current fiscal environment, in building the fiscal year 2012 budget, all DHS components identified savings associated with the Department's 33 efficiency review initiatives, and we cut administration and overhead, including my own office's budget, by more than \$800 million. Savings were realized through efficiencies in acquisition, asset, and real property management, as well as employee vetting and credentialing, hiring and on-boarding, and information technology. We cut professional services contracts, travel, and nonmission-critical training.

We also delayed construction of FEMA at the new DHS headquarters at St. Elizabeths and deferred office collocations, as well as building maintenance and enhancements.

My written statement includes a comprehensive list of the operational priorities in the budget request, and today I would like to highlight a few of them for you here, even as I request that the full statement be admitted in your record.

First, preventing terrorism and enhancing security was the founding mission of DHS. It remains our top priority today. This budget safeguards transportation modes through a layered detection system, including the deployment of additional transportation security officers, behavioral detection officers, canine teams, and advanced imaging technology machines at domestic airports while expanding watch list vetting through the secure flight program and enhancing screening and targeting of international travelers before they board U.S.-bound flights through the immigration advisory program.

The budget also strengthens surface transportation security by supporting 12 new multimodal VIPR teams. The acronym stands for “Visible Intermodal Prevention and Response.” These teams conduct operations throughout the transportation sector to prevent potential terrorist activity.

The request also provides funding for the Securing the Cities program to protect our highest risk cities from a radiological or a nuclear attack and makes a significant investment in the National Bio- and Agro-Defense Facility which will provide enhanced diagnostic capabilities to protect our country from foreign animal and emerging diseases.

The request expands support for the national network of State and local fusion centers to enhance baseline capabilities and local law enforcement with the tools they need to address threats in their communities.

Now, to secure and manage our borders, the request continues the administration’s historic border security efforts by supporting 21,370 Border Patrol agents and 21,186 U.S. Customs and Border Protection officers, both all-time highs. The budget also includes \$242 million for the continued deployment of proven, effective surveillance technology along the highest trafficked areas of the Southwest Border to better meet the operational requirements of our agents on the front lines.

For the Northern Border, this budget request supports investments in technology tailored to the maritime and cold weather environment, including proven standalone technology to provide immediate operational benefits.

And for our Nation’s maritime borders, this budget includes funding to continue the essential national security cutter program and makes historic investments to recapitalize the Coast Guard’s aging assets, including 6 fast response cutters, 40 response boats, as well as a sizable investment in the renovation and restoration of aging shore facilities.

The budget request also continues the Department’s focus on smart and effective enforcement of our U.S. immigration laws, while streamlining and facilitating the legal immigration process. Building on our record over the past 2 years, the Department will continue to prioritize the identification and removal of criminal aliens who pose a threat to public safety, and target employers who knowingly and repeatedly break the law. This request enables ICE to fund 33,400 detention beds, remove more than 200,000 criminal aliens, and deploy Secure Communities to 96 percent of all jurisdictions nationally in fiscal year 2012, while promoting compliance with worksite-related laws through criminal prosecution of egregious employers. Form I-9 inspections and continued expansion and enhancements of E-Verify are included.

The request funds integration efforts, including programs supporting English-language and citizenship education, and continues detention reform efforts currently underway.

Now, to safeguard and secure cyberspace, the budget increases resources to identify and reduce vulnerabilities in our Nation’s key cyber networks. It includes significant investments to expedite the deployment of Einstein 3 to prevent and detect intrusions on Government computer systems, increase Federal network security of

large and small agencies, and continue to develop a robust cybersecurity workforce to protect against and respond to cybersecurity threats. The budget also focuses on combating cyber crime and preventing attacks against United States critical infrastructure.

Now, to ensure resilience to disasters, as you mentioned, Madam Chair, the budget request focuses on moving resources out of Washington, DC, and into the hands of State and local responders who are often best positioned to detect and respond to terrorism, to natural disasters, and to other threats by sustaining Federal funding for State and local preparedness grants, providing \$3.8 billion in fiscal year 2012. The funding also includes \$670 million for assistance to firefighter grants, including \$420 million to rehire an estimated 2,300 laid-off firefighters and retain veteran first responders.

Now, to lead and support essential national security and economic security efforts, the budget expands the Coast Guard's operational capacity by funding 50,682 military and civilian positions and establishing the Coast Guard's first incident management assistance team, which will be deployed rapidly to support incidents of national significance.

It also continues to support ICE and CBP's enforcement and investigative efforts to protect U.S. intellectual property rights, as well as the Secret Service's state-of-the-art forensic support for the National Center for Missing and Exploited Children.

Madam Chair, this budget is the culmination of a major, first-of-its-kind effort by the Department through the Quadrennial Homeland Security Review and the associated Bottom-Up Review to align our resources with a comprehensive strategy to ensure a safe, secure, and resilient homeland while making an unprecedented commitment to fiscal discipline.

PREPARED STATEMENT

I would be remiss, however, if I did not note all of this progress is at risk in the continuing resolution passed by the House. This is the full fiscal year 2011 resolution. That proposal cuts technology investments and security improvements on the Southwest and Northern Borders. It cuts aviation security measures. It cuts funding to sustain the progress that has been made in enforcing the Nation's immigration laws. It cuts critical cybersecurity tools and operations. It cuts intelligence personnel. It cuts Coast Guard funding to support our war efforts abroad, and it cuts grants that support counter-terrorism and disaster response capabilities at the local level.

Chairman Landrieu, Senator Coats, members of the subcommittee, thank you for this opportunity to testify. I am happy to continue to answer your questions.

[The prepared statement follows:]

PREPARED STATEMENT OF SECRETARY JANET NAPOLITANO

Chairman Landrieu, Ranking Member Coats, and members of the subcommittee: Let me begin by saying thank you to this subcommittee for the strong support you have provided me and the Department over the past 2 years. I look forward to continuing to work with you in the coming year to protect the homeland and the American people.

I am pleased to appear before the subcommittee today to present President Obama's fiscal year 2012 budget request for the Department of Homeland Security (DHS).

The demands on DHS have never been greater and the threats we face pose new challenges that require an innovative and focused response. Today's threat picture features an adversary who evolves and adapts quickly and who is determined to strike us here at home—from the aviation system and the global supply chain to surface transportation systems, critical infrastructure, and cyber networks. The Department's fiscal year 2012 budget allows us to continue to meet these evolving threats and challenges by prioritizing our essential operational requirements—while reflecting an unprecedented commitment to fiscal discipline that maximizes the effectiveness of every security dollar we receive.

Reflecting the current economic environment, we are preserving essential front-line operations and bolstering our operational strength by decreasing administration and overhead, including the overall budget for the Office of the Secretary and Executive Management. All DHS Components identified reductions associated with the Efficiency Review initiatives currently underway as well as administrative savings totaling nearly \$800 million to strengthen mission-critical activities across the Department. Savings were accomplished through efficiencies in acquisition, asset, and real property management as well as employee vetting/credentialing, hiring/onboarding, and information technology; and administrative savings through reductions to professional services contracts, printing, supplies and materials, travel, and training. The Department also proposes to delay construction of the Federal Emergency Management Agency (FEMA) headquarters at St. Elizabeths as well as the deferral of other office colocations, and building maintenance and enhancements to prioritize frontline security operations.

FISCAL YEAR 2012 BUDGET REQUEST

The fiscal year 2012 budget request for DHS is \$57.0 billion in total funding, \$47.4 billion in gross discretionary funding, and \$43.2 billion in net discretionary funding.¹

DHS's fiscal year 2012 budget request is the culmination of a major, first of its kind effort undertaken by the Department to align DHS resources with a comprehensive strategy to meet our Nation's homeland security needs. Last year, DHS completed the first ever Quadrennial Homeland Security Review (QHSR), which established a unified, strategic framework for Homeland Security missions and goals, as well as the first ever Bottom-Up Review (BUR), which aligned DHS' programmatic activities and organizational structure to better serve those missions and goals. The third and final step of this process is the fiscal year 2012 budget submission, which begins the next phase in strengthening DHS efforts to ensure a safe, secure, and resilient homeland.

This process identified six DHS missions, each of which is strengthened by this budget:

Mission 1: Preventing Terrorism and Enhancing Security.—Protecting the United States from terrorism is the cornerstone of Homeland Security. DHS's counterterrorism responsibilities focus on three goals: preventing terrorist attacks; preventing the unauthorized acquisition, importation, movement, or use of chemical, biological, radiological, and nuclear materials and capabilities within the United States; and reducing the vulnerability of critical infrastructure and key resources, essential leadership, and major events to terrorist attacks and other hazards.

Mission 2: Securing and Managing Our Borders.—DHS secures the Nation's air, land, and sea borders to prevent illegal activity while facilitating lawful travel and trade. The Department's border security and management efforts focus on three interrelated goals: effectively securing U.S. air, land, and sea borders; safeguarding and streamlining lawful trade and travel; and disrupting and dismantling transnational criminal and terrorist organizations.

Mission 3: Enforcing and Administering Our Immigration Laws.—DHS is focused on smart and effective enforcement of U.S. immigration laws while streamlining and facilitating the legal immigration process. The Department has fundamentally reformed immigration enforcement, focusing on identifying and removing criminal aliens who pose a threat to public safety and targeting employers who knowingly and repeatedly break the law.

Mission 4: Safeguarding and Securing Cyberspace.—By statute and presidential directive, DHS has the lead for the Federal Government to secure civilian govern-

¹ For purposes of comparison to prior year funding levels, funding for overseas contingency operations and National Science Foundation transfers are not included in these figures.

ment computer systems and works with industry and State, local, tribal, and territorial governments to secure critical infrastructure and information systems. DHS analyzes and reduces cyber threats and vulnerabilities; distributes threat warnings; and coordinates the response to cyber incidents to ensure that our computers, networks, and cyber systems remain safe.

Mission 5: Ensuring Resilience to Disasters.—DHS provides the coordinated, comprehensive Federal response in the event of a terrorist attack, natural disaster or other large-scale emergency while working with Federal, State, local, and private sector partners to ensure a swift and effective recovery effort. The Department's efforts to build a ready and resilient Nation include fostering a community-oriented approach; bolstering information sharing; improving the capability to plan; and providing grants and training to our Homeland Security and law enforcement partners.

Mission 6: Providing Essential Support to National and Economic Security.—DHS leads and supports many activities that provide essential support to national and economic security including, but not limited to: maximizing collection of customs revenue; maintaining the safety of the marine transportation system; preventing the exploitation of children; providing law enforcement training; and coordinating the Federal Government's response to global intellectual property theft. DHS contributes in many ways to these elements of broader U.S. national and economic security while fulfilling its other five Homeland Security missions.

The following are highlights of the fiscal year 2012 budget:

PREVENTING TERRORISM AND ENHANCING SECURITY

Advanced Imaging Technology (AIT).—\$105.2 million and 535 positions are included for the Transportation Security Administration (TSA) to purchase, install, and operate 275 AITs at airport checkpoints. The fiscal year 2012 request, combined with prior requests, will result in 1,275 AIT units deployed by the end of 2012. The requested funding covers the cost of new Transportation Screening officers and managers to operate the new AITs, as well as the associated support and airport management costs. Continuing to increase AIT deployments while ensuring privacy safeguards are in place is critical to address the current threat by safely screening passengers for metallic and nonmetallic threats—including weapons, explosives and other objects concealed under layers of clothing.

Explosives Detection Systems (EDS).—\$273 million is requested to support the recapitalization and deployment of state-of-the-art EDS for checked baggage to efficiently screen baggage for explosives, reducing the number of rescans and physical bag searches. Beginning in fiscal year 2012, more than 800 EDS in our largest airports will exceed their planned 10-year service life.

Assistant Field Security Directors-Law Enforcement (AFSD-LEs).—Requested funding of \$22.5 million supports 82 AFSD-LEs currently deployed and provides 22 additional AFSD-LEs for major airports, where they serve as the primary liaison to local law enforcement as AIT expansion continues.

Federal Air Marshal Service (FAMS).—The fiscal year 2012 budget requests funds to maintain the FAMS surge deployment levels for domestic and international flight coverage that began in response to the attempted terrorist attack on December 25, 2009. Members of the FAMS, TSA's law enforcement entity, are deployed on flights around the world and the United States based on risk in order to detect, deter, and defeat hostile acts targeting U.S. air carriers, airports, passengers, and crews.

Enhanced Watchlist Vetting.—\$12.4 million is proposed for maintaining the expanded watchlist vetting initiative, which, through the Secure Flight program, enables TSA to identify individuals who may present a threat to passenger air travel. Through Secure Flight, TSA prescreens passenger name, date of birth, and gender against terrorist watchlists before passengers receive their boarding passes. In addition to facilitating secure travel for all passengers, the program helps prevent the misidentification of passengers who have names similar to individuals on government watchlists.

Immigration Advisory Program (IAP).—A total request of \$14.1 million will permit the IAP to expand in Paris, Abu Dhabi, Dubai, and Amman. IAP is a part of Custom and Border Protection's (CBP) layered risk-based security approach, which includes working with international partners to post CBP officers at foreign airports and use advanced targeting and passenger analysis information to identify high-risk travelers at foreign airports before they board U.S.-bound flights.

Behavior Detection Officers (BDOs).—The fiscal year 2012 budget request of \$236.9 million funds 3,336 BDOs, which includes 350 new positions. BDOs serve as an additional layer of security in airports by providing a nonintrusive means of identifying individuals who may pose a risk of terrorism or criminal activity.

Canine Teams.—Requested funding of \$125.7 million allows TSA to sustain the deployment of 900 canine teams supported by reallocations made under the continuing resolution, providing an important layer of security to complement passenger checkpoint screening at airports, assist in air cargo screening and enhance security in the mass transit environment.

Visible Intermodal Prevention and Response (VIPR) Teams.—\$109 million requested supports 37 VIPR teams and includes 12 new multi-modal VIPR Teams proposed in the fiscal year 2012 request in addition to the 10 existing teams in Aviation and the 15 VIPR teams dedicated to surface transportation added in the fiscal year 2010 budget. VIPR teams are comprised of personnel with expertise in inspection, behavior detection, security screening, and law enforcement for random, unpredictable deployments throughout the transportation sector to deter potential terrorist and criminal acts.

Passenger Security Fee.—The fiscal year 2012 budget reflects a proposal to increase the Aviation Passenger Security Fee by \$1.50 per enplanement beginning in 2012. The Aviation Passenger Security fee has not changed since the TSA was established following the events of 9/11, even though the overall cost of aviation security has grown by more than 400 percent. The administration's proposal makes progress towards fulfilling the intent of the Aviation and Transportation Security Act to cover the costs of aviation security through fees and not by the general taxpayers.

BioWatch Gen 1/2.—\$90 million is requested to continue operating the Gen 1/2 BioWatch detection network, a federally managed, locally operated, nationwide bio-surveillance system designed to detect the intentional release of aerosolized biological agents in more than 30 cities.

BioWatch Gen-3.—The fiscal year 2012 budget provides \$25 million to continue Gen-3 development, which is expected to significantly reduce the time between a release of a biothreat agent and confirmation of that release by BioWatch technology. Operational testing and evaluation of Gen-3 technology will begin in one of four test cities in fiscal year 2012 with full deployment expected in fiscal year 2014.

Securing the Cities.—\$27 million is requested for Securing the Cities to continue the build-out of the domestic portion of the global nuclear detection architecture, the multi-layered system of detection technologies, programs, and guidelines designed to enhance the Nation's ability to detect and prevent a radiological or nuclear attack in our highest risk cities.

Radiological/Nuclear Detection Systems.—The fiscal year 2012 budget requests \$57 million for the procurement and deployment of radiation portal monitors and human portable radiation detection systems, providing vital detection equipment to CBP and the U.S. Coast Guard to scan for radiological and nuclear threats.

Countermeasures and 2012 Presidential Candidate Nominee Protection.—The fiscal year 2012 request funds critical Secret Service operations and countermeasures to protect the first family and visiting dignitaries, including the 2012 presidential campaign and three anticipated National Special Security Events (NSSEs). The budget also restores the Secret Service's base funding—supporting the replacement of protective equipment, vehicles, training of personnel, and other infrastructure to allow the Secret Service to improve the execution of its protective and investigatory missions.

National Network of Fusion Centers.—The fiscal year 2012 budget expands support for the national network of fusion centers in order to provide State and local law enforcement with the tools they need to address threats in their communities. The request focuses on integrating and coordinating cross-department and cross-government interaction with fusion centers focused on enhancing baseline capabilities.

State and Local Law Enforcement Training.—The fiscal year 2012 budget provides funding to train 64,000 individual Federal, State, and local law enforcement personnel through the Federal Law Enforcement Training Center and its total budget of \$276 million.

National Bio- and Agro-Defense Facility (NBAF).—\$150 million is requested to begin construction of the NBAF, which will serve as a new, state-of-the-art biosafety level 3 and 4 facility. Work performed at NBAF will lead to the development of vaccines and antivirals and enhanced diagnostic capabilities for protecting our country from numerous foreign animal and emerging diseases.

SECURING AND MANAGING OUR BORDERS

CBP Law Enforcement.—The fiscal year 2012 budget supports 21,370 Border Patrol agents and 21,186 CBP officers at our ports of entry who work 24/7 with State, local, and Federal law enforcement in targeting illicit networks trafficking in people, drugs, illegal weapons, and money. This reflects the largest deployment of law en-

forcement officers to the front line in the agency's history. The request annualizes positions supported by the fiscal year 2010 Emergency Border Security Supplemental for the Southwest Border, including 1,000 Border Patrol agents and 250 CBP officers. Funding is provided to support 300 new CBP officers above the fiscal year 2011 budget and additional canine assets to support Port of Entry operations. The request supports the mobile response surge teams created with the supplemental funding to respond rapidly to emergent situations without depleting Border Patrol staffing from other locations.

New Southwest Border Technology.—\$242 million is requested to support the continued deployment of proven, effective surveillance technology along the highest trafficked areas of the Southwest Border. Funds will be used to procure and deploy commercially available technology tailored to the operational requirements of the Border Patrol, distinct terrain, and population density of each border region. These funds will allow CBP to fully deploy a mix of integrated fixed towers and other mobile equipment in three of the five Border Patrol stations' areas of responsibility in Arizona.

Northern Border Technology.—The request includes \$55 million to support investments in technology systems which address security needs for the Northern Border maritime and cold weather environment, as well as innovative technology pilots. It will also deploy proven, standalone technology that provides immediate operational benefits. These demonstrations and deployments explore how best to integrate various sensors, border security organizations, and mission operations in order to optimize border security in this challenging environment.

CBP Journeyman.—The request includes \$229 million to fully fund the increase in journeyman grade level for frontline CBP officers, Border Patrol agents, and CBP agricultural specialists from GS-11 to GS-12.

Tactical Communications (TACCOM).—The fiscal year 2012 budget includes \$40 million to continue the transition of the TACCOM program to a robust, open architecture system that will increase interoperability with other law enforcement, expand coverage, and improve agent safety in the Houlton, El Paso, Laredo, and Rio Grande Valley sectors.

National Targeting Center-Passenger (NTC-P).—A total of \$47 million is requested to enhance CBP's ability to interdict dangerous individuals or terrorists traveling from foreign locations before boarding flights destined for the United States. The funds will be used to hire additional staff and implement enhancements in targeting priorities.

U.S. Coast Guard Recapitalization.—The fiscal year 2012 request fully funds the fifth national security cutter (NSC), supports 40 response boats and 6 fast response cutters, as well as a sizable investment in the renovation and restoration of shore facilities. The budget also provides resources to ensure that the Coast Guard's aviation fleet is mission-ready through the acquisition of two maritime patrol aircraft, one HH-60 helicopter, and conversion and sustainment projects of multiple aircraft. Funding for the NSC underscores the Department's support of this program which is important to the Coast Guard's long-term recapitalization effort and, most importantly, to allow the Coast Guard to replace its aged, obsolete high endurance cutter fleet as quickly as possible. The total request for U.S. Coast Guard acquisition, construction, and improvements is \$1.4 billion.

Maritime Safety and Response.—\$115.5 million remains in Coast Guard's base resources for 11 maritime safety and security teams and their associated 921 personnel, who conduct port security activities and provide support to NSSEs.

ENFORCING AND ADMINISTERING OUR IMMIGRATION LAWS

Detention Beds.—The fiscal year 2012 budget increases U.S. Immigration and Customs Enforcement (ICE) Custody Operations funding by \$157.7 million to support 33,400 detention beds and remove more than 200,000 criminal aliens in fiscal year 2012.

Detention Reform.—ICE plans to continue building on its detention reform efforts in fiscal year 2012 by improving detainee access to quality healthcare, reducing the average length of stay, and facilitating access to family members and legal representation by adding functionality to the recently released online detainee locator system.

Worksite Enforcement.—Requested funds continue the Department's focus on worksite enforcement, promoting compliance with worksite-related laws through criminal prosecutions of egregious employers, Form I-9 inspections, civil fines, and debarment, as well as education and compliance tools.

E-Verify.—The fiscal year 2012 request continues support for E-Verify operations and enhancements, including continued funding for new monitoring, compliance,

and outreach positions necessitated by program expansion. The continued success of E-Verify demonstrated by recent independent reports reflect the administration's commitment to smart, tough, and effective strategies that build a strong foundation upon which immigrants can exercise their rights and responsibilities as Americans.

Secure Communities.—A total of \$184 million is requested for Secure Communities—which uses biometric information and services to identify and remove criminal aliens in State prisons and local jails. The \$64 million program increase will expand deployment to 96 percent of all jurisdictions nationally in fiscal year 2012 and provide resources to confirm the identification of an estimated 199,000 more criminal aliens through interoperability in fiscal year 2012 than fiscal year 2010 and transport more than 44,000 criminal aliens from State and local jails into the custody of ICE following the completion of their sentences. ICE will work with DHS's Office of Civil Rights and Civil Liberties and the Department of Justice to develop a robust oversight and evaluation process of Secure Communities and to provide training to State and local law enforcement. Secure Communities is on track for nationwide deployment by 2013.

Visa Security Program.—The budget requests \$29 million to continue the Visa Security Program at current locations. This program enhances national security by preventing terrorists, criminals, and other ineligible applicants from receiving visas.

Immigrant Integration.—The fiscal year 2012 request expands U.S. Citizenship and Immigration Services' (USCIS) effort to support immigrant integration efforts, including funding for new programs supporting English language acquisition and citizenship education.

SAVE.—The fiscal year 2012 request continues support for USCIS SAVE operations and enhancements to assist State, local, and Federal agencies in determining individuals' eligibility for public benefits based on their immigration status.

USCIS Business Transformation.—The fiscal year 2012 request continues the multi-year effort to transform USCIS from a paper-based filing system to a customer-focused electronic filing system.

SAFEGUARDING AND SECURING CYBERSPACE

Federal Network Protection.—\$233.6 million is requested to expedite the deployment of Einstein 3 to prevent and detect intrusions on computer systems and to upgrade the National Cyber Security Protection System, building an intrusion detection capability and analysis capabilities to protect Federal networks.

Federal IT Security Assessments.—A total of \$40.9 million in requested funds will support the Department's efforts to strengthen Federal network security of large and small agencies by conducting an estimated 66 network assessments to improve security across the Federal executive branch.

Cybersecurity Workforce Needs.—\$24.5 million is proposed to provide high-quality, cost-effective virtual cybersecurity education and training to develop and grow a robust cybersecurity workforce that is able to protect against and respond to national cybersecurity threats and hazards.

Cyber Investigations.—The fiscal year 2012 budget continues to support cyber investigations conducted through the Secret Service and ICE, targeting large-scale producers and distributors of child pornography and preventing attacks against U.S. critical infrastructure through financial crimes task forces.

Cyber Mission Integration.—The fiscal year 2012 request includes \$1.3 million to enable DHS to coordinate national cybersecurity operations and interface with the U.S. Department of Defense's (DoD) National Security Agency (NSA) at Fort Meade, Maryland. This funding will support a landmark memorandum of agreement signed by Secretary Napolitano and Secretary of Defense Robert Gates that aligns and enhances America's capabilities to protect against threats to critical civilian and military computer systems and networks.

Cybersecurity Research.—The fiscal year 2012 request includes an increase of \$18 million for the Comprehensive National Cybersecurity Initiative to support research and development projects focused on strengthening the Nation's cybersecurity.

ENSURING RESILIENCE TO DISASTERS

State and Local Grants.—The fiscal year 2012 request sustains Federal funding for State and local preparedness grants totaling more than \$3.8 billion, highlighting the Department's commitment to moving resources out of Washington, DC and into the hands of State and local first responders who are often best positioned to detect and respond to terrorism, other threats, and natural disasters.

Assistance to Firefighters Grants.—The fiscal year 2012 request includes \$670 million. Included in this amount are \$420 million for Staffing for Adequate Fire and Emergency Response (SAFER) grants to rehire laid off firefighters and retain vet-

eran first responders—totaling 2,300 firefighter positions—and \$250 million for equipment, training, vehicles, and related materials.

Disaster Relief Fund (DRF).—\$1.8 billion is requested for the DRF to allow FEMA to continue to address the impacts of a disaster on individuals and communities across the Nation. The DRF provides a significant portion of the total Federal response to victims in presidentially declared disasters or emergencies.

Regional Catastrophic Event Planning.—\$8.5 million is requested to continue development of catastrophic plans, with a focus on plans for response to biological events and earthquakes.

National Exercises.—FEMA's participation in National Level Exercise-12, an exercise to test FEMA's ability to respond to a catastrophic cyber attack, is funded with \$3 million through the request.

Emergency Management Oversight.—The fiscal year 2012 request includes \$20 million for the Office of the Inspector General to continue its Emergency Management Oversight operations.

PROVIDING ESSENTIAL SUPPORT TO NATIONAL AND ECONOMIC SECURITY

Patrolling the Exclusive Economic Zone.—The Coast Guard patrols the U.S. Exclusive Economic Zone boundary areas to reduce the threat of foreign poaching of U.S. fish stocks and ensure compliance with international living marine resource agreements. The budget includes \$47 million to extend the service life of five Medium Endurance Cutters critical in support of this mission.

U.S. Coast Guard Staffing.—The request strengthens the Coast Guard's operational capacity by funding a total of 50,682 civilian and military personnel in fiscal year 2012.

Enhancing Maritime Safety.—The fiscal year 2012 budget requests \$686.3 million and 4,717 FTEs for the Coast Guard's maritime safety activities. The fiscal year 2012 budget provides 105 new Marine Safety Inspectors and Investigators to staff ship inspections and post-incident investigations.

Enhancing Marine Environmental Protection and Response.—The fiscal year 2012 budget requests \$225.2 million and 1,362 FTE to enable the Coast Guard to conduct Marine Environmental Response. This includes 87 new environmental response personnel and creates the Coast Guard's first incident management assistance team, a highly trained team that will be deployed rapidly to augment the Coast Guard command structure when an incident of national significance occurs.

Investigate Cultural Antiquity Trafficking and Coordinate Repatriation.—The fiscal year 2012 budget continues to support ICE seizures and repatriation of cultural property, art and antiquities illegally imported into the United States and the investigation of illegal trafficking of artwork, especially works that have been reported lost or stolen.

Forensic Support for Missing and Exploited Children.—Funding is requested for the Secret Service to provide forensic support to the National Center for Missing and Exploited Children, which provides state-of-the-art forensics support for investigations involving missing and exploited children and grant funds for activities related to the investigations of missing and exploited children.

Collect Customs Revenue.—Funds are requested to support CBP's role as a revenue collector for the U.S. Treasury—customs revenue remains the second-largest source of revenue for the U.S. Government. Customs and Border Protection has set revenue collection as a priority trade issue to ensure effective internal controls that protect the duties and taxes (more than \$29 billion in 2009) collected for the U.S. Government.

Protect U.S. Intellectual Property Rights.—The fiscal year 2012 budget request funds to support CBP's enforcement program to prevent trade in counterfeit and pirated goods, and enforce exclusion orders on patent-infringing and other intellectual property rights violative goods. The ICE HSI Intellectual Property Rights (IPR) Center investigates the smuggling and distribution of counterfeit goods and products that pose risks to public safety and security. Counterfeit pharmaceuticals and critical technology components, such as computer chips for defense systems and airplane equipment, were among the top seized commodities in IPR investigations.

MATURING AND STRENGTHENING THE HOMELAND SECURITY ENTERPRISE

Maturing and strengthening the Homeland Security enterprise—the collective efforts and shared responsibilities of Federal, State, local, tribal, territorial, non-governmental, and private-sector partners, as well as individuals, families, and communities—is critical to the Department's success in carrying out its core missions and operational objectives. This includes enhancing shared awareness of risks and threats, building capable communities, and fostering innovative approaches and so-

lutions through cutting-edge science and technology, while continuing to foster a culture of efficiency, sustainability in accordance with Executive Order 13514 and fiscal responsibility and streamline management across the Department.

While the Department proposes significant cuts to administrative support across all components in order to maintain frontline operations, the following activities are supported through the fiscal year 2012 budget:

St. Elizabeths.—\$159.7 million is requested for the St. Elizabeths project. This funding enables DHS to complete the Coast Guard headquarters facility and to continue work on the National Operations Center. The request, however, will defer the FEMA headquarters consolidation.

Transformation and Systems Consolidation (TASC).—The fiscal year 2012 budget proposes \$11 million to fund the TASC program, which supports the modernization of the Department's financial, asset, and acquisition management systems—a key priority for the Department and a step towards addressing recommendations on the GAO high-risk list.

Acquisition Workforce.—\$24.2 million in requested funds will increase the Department's acquisition workforce capacity by 150 positions, including additional systems engineers, program managers, logisticians and business cost estimators, to ensure operational requirements are properly developed and included in DHS contracts and to provide greater oversight and accountability. This too, is consistent with previous recommendations from the Government Accountability Office and Inspector General.

Information Security and Infrastructure.—\$32.3 million is requested to establish a unified email network for DHS-wide use, and provide Single Sign-On and other capabilities. These activities will leverage technologies to strengthen DHS operations and enhance communications with Federal, State, local, and private sector partners.

Coast Guard Housing and Child Care.—The health and welfare of military families is the heart of Coast Guard operational readiness. The fiscal year 2012 budget includes \$29 million to address critical housing shortfalls and improve access to affordable, quality childcare. These initiatives will ensure Coast Guard members can maintain both strong families and a high state of readiness.

CONCLUSION

The fiscal year 2012 budget proposal reflects this administration's strong commitment to protecting the homeland and the American people through the effective and efficient use of DHS resources. As outlined in my testimony today, the Department will continue to build upon past successes in several areas including securing U.S. air, land, and sea borders; safeguarding lawful trade and travel; securing Federal networks; and disrupting and dismantling transnational criminal and terrorist organizations that engage in cross-border criminal activity while maximizing every taxpayer dollar we receive.

Thank you for inviting me to appear before you today. I look forward to answering your questions and to working with you on the Department's fiscal year 2012 budget request and other Homeland Security issues.

Senator LANDRIEU. Thank you, Madam Secretary.

And since I have asked one question, I am just going to ask two additional ones and then turn it over to my co-chair, to the ranking member.

CONTINUING RESOLUTION

I want to follow up on just your last statement—the House recently passed a continuing resolution that cut funding by \$2.5 billion in this Department, which is 6 percent below the 2010 budget. As you stated, it cuts port security grants, deep cuts to the Coast Guard, which are particularly troubling to myself and I think Senator Cochran as well. And there are other aspects.

Could you give a little bit more detail, if we are not able to modify some of these cuts, what consequences it will actually have in your Department?

Secretary NAPOLITANO. Madam Chair, here are a few of the details. It cuts the number of AIT machines we can deploy to our Nation's airports. And these are necessary because our adversaries, al

Qaeda/al Qaeda-related, continue to seek aviation as a target and continue to target it by means other than something that would be picked only by a magnetometer. So we need to move to the next generation, and that is the AIT machine. It cuts those by 250 and the 500 requested, cuts the number of portable ETD machines, explosive trace detection machines, by half. It cuts the number of canine teams by two-thirds. It cuts the personnel responsible for background investigations, intelligence redress, and air cargo and surface inspections. It will probably result in an increase in wait times for passengers in the air environment, and those could be significant.

It cuts the deployment of intelligence personnel to State and local fusion centers. This is a network of 72 centers that we have installed as really the portals of entry through which intelligence can be shared at the Secret and above level out to our States and localities, and intelligence can be received back so that we really have a Homeland Security intelligence capability. It cuts that very, very deeply.

In addition, it cuts funding for at least 250 ICE agents along the border. Agent Zapata, by the way, the agent who was just murdered in Mexico, was an ICE special agent. It eliminates or if the cuts are annualized in the 2012—and that is a concern I have that the House continuing resolution for 2011 then becomes the budget for 2012. If it does that, it will not annualize the additional Border Patrol agents this Congress approved of in a supplemental not too long ago. So those will go away.

I could go into more detail, Madam Chair, but you get a sense of what this would do to us.

Senator LANDRIEU. It gives us a sense of what the challenge is. And as I was with you just yesterday at Georgetown for that really remarkable gathering of the past two Homeland Security Secretaries, as we saw, Secretary Ridge, Secretary Chertoff, and yourself there, it reminded me that this was the largest reorganization of the Federal Government since Harry Truman organized the aspects of the military, the branches of the military, into the Department of Defense. And so this is the youngest of all the Federal Departments.

So as we are looking, Senator Coats, for efficiencies, which we all want to look for in streamlining, we have to be mindful that we are building, not streamlining this Department. We are building and potentially streamlining, but we are not taking down. We are building this agency, and that takes investments and resources.

AIRLINE FEES

My final question, if you could answer this very shortly. I have been becoming very concerned with the airlines and the charges that they are charging to passengers. And particularly, I know this is under the Department of Commerce, but under our jurisdiction is the way it affects TSA. And I have asked the staff to get some information.

Checked baggage fees are increasing. It looks like, the cost to TSA is also increasing because people do not want to pay the fees. So they are not checking bags, putting more on the planes, slowing

down actually the seating, of course. But I understand that it is a \$250 million annual cost to TSA because of those extra bags.

My question is, do the taxpayers have to pick up this cost or should we be looking to the airlines to give us some of the profits that they are making from these fees to offset the cost to the taxpayer?

Secretary NAPOLITANO. Madam Chair, the answer is that when you have to pay to check a bag, it increases carry-on luggage, and that means that there is more to inspect at the gate and so forth for passengers getting on the planes. We do have an estimate. That is roughly \$260 million.

One of the reasons we requested the ability to charge a security fee for travelers—I think, Senator Coats, you referenced that in your statement—was because we need to be able to pay for this additional security that TSA must have. And if we do not have the ability to have a security fee, which by the way has not been adjusted since 2002, that is at least a \$600 million bite that we have to eat somewhere. And as you can tell from my opening statement, everywhere you hit in this Department, it is going to have an operational impact.

Senator LANDRIEU. Thank you, Madam Secretary.

Senator Coats.

Senator COATS. Thank you.

CONTINUING RESOLUTION

I have got some specific questions here, but really in looking at the larger picture, the reality is that we do have this significant deficit problem and it is going to be addressed one way or another. The Congress can address it as it has done through current efforts on the continuing resolution for the remainder of the current fiscal year, but also structuring how next year's functions of Government will be funded.

The reality is, I think, that no one is going to get everything that they would like to get. And the question I have for you is—and I know you have scrubbed your budget—but if you start with the assumption that you may not get in your budget all the requests that have been made, have you scrubbed the system to, in a sense, categorize those requests? If you have to come back to us and say, okay, this is all we are going to get—have you scrubbed your budget in a way that you could say we deem these to be absolutely essential? We have the next category that are very important but not absolutely essential; another category that says these potentially can be deferred until revenues increase or we are able to do better with the budget; and these are ones that we think could be nice to have but not really necessary to have and could potentially be terminated to gain those savings. It might be accompanied with, say, a provision which you just discussed, an increase in fees on the enplaning.

But I guess my question is, have you done this? Do you contemplate having to move to a plan B should the Congress not be able to fund the budget as presented? And if you have, can you share that with us? And if you have not, is that something in the plans?

Secretary NAPOLITANO. Well, Senator Coats, we went through that analysis in working with OMB on what the President's budget request would be and finding places or things that could be put off or delayed.

For example, postponing the move to a real Department headquarters at St. Elizabeths was something that we recommended, going through kind of the analysis you just suggested. Now, if you saw where our headquarters are now and the office that I have and others have, you would know that we made a tough choice there. That means that we cannot have all our components collocated. It means that from a managerial standpoint, we still are spread out. We postponed all collocations in other cities across the country because of the associated costs of moving people, and that has a managerial impact to it as well.

So I believe the President's budget reflects the analysis that you have just suggested and that real choices have been made in it already.

BUDGET

Senator COATS. Well, I am sure that is what the President's budget projects and thinks, but I mean, obviously, we are going to have a congressional budget I hope. And we are certainly going to have congressional appropriations, and they may not match what the President has proposed. Every agency is going to come here and say exactly what you have said. We are cut to the bone. The President's budget is as low as we can go. The reality in this Congress is that we are going to appropriate—I believe, going to end up appropriating less than what that budget asks for.

And so it seems to me that it would be prudent for every agency to simply kind of red team your current budget and basically say if what happens probably happens, then where do we go? Will we have something that we can bring back to the Congress and present and say we do not like it, but these are the consequences, but this is what we will have to do if we come in at this number?

Secretary NAPOLITANO. We look forward to, Senator, to working with you on the budget. I just would respectfully suggest that this Department is somewhat unique. It is new. It is virtually all operations. And so when you look at this budget, it really is tied to the five priorities I identified for you in my opening statement.

Senator COATS. Well, I agree with that. I mean, along with national defense, homeland security, a couple of others are essential functions of the U.S. Government. I could not agree more. But there just are fiscal realities that we have to deal with, and I think right now the method going forward is to take a look at every area to see if we can find efficiencies.

Doing as much or more with less is something, again, that all of America has had to do in these last 2 years, and it is easier for some than others. But everyone has been forced to make those hard decisions, and I think in this case the reality is that there will probably be some hard decisions that will have to be made.

I do not look forward to working on this together; it is not something either of us relish, but I think it is something that we are going to have to do.

Secretary NAPOLITANO. Senator, I think, first of all, we are always willing to supply information. As you go through the budget request and have questions about things, we are more than happy to work with you on that.

Senator COATS. My time is about to expire. Given the fact that we have a vote coming up and some other members may want to talk, I will wait.

Senator LANDRIEU. Thank you, Senator Coats.

Senator Cochran.

Senator COCHRAN. Madam Chairman, thank you. Congratulations on your leadership of this subcommittee.

Madam Secretary, welcome. We look forward to working closely with you to identify our budget needs and to try to respond to them in a thoughtful and expeditious manner.

One of the difficulties I know that you face is the lack of predictability about when funds are available for this program or that. I wonder if you could share with us some specific examples of what problems you might encounter if we do not move quickly to provide you certainty with respect to your budget needs.

Secretary NAPOLITANO. Well, I think from a management perspective, managing by small continuing resolutions is very difficult. It affects your ability to undertake key acquisitions. It affects your ability to hire personnel. It affects your ability to make investments in things that you kind of think will be ultimately in the budget, but those funds are not yet available. So from a management perspective, it makes a difficult management job even more difficult.

COAST GUARD SHIPBUILDING

Senator COCHRAN. One of the things we are proud of in our State is the fact we have a shipbuilding capability on the Mississippi gulf coast at Pascagoula, and part of the mission there is to fulfill contracts that are made with the Department that you lead for Coast Guard cutters. What is the status of our shipbuilding progress in meeting those needs, and what can we do to work more effectively with you predicting what the future is going to hold?

Secretary NAPOLITANO. Here is what we are requesting for the Coast Guard, that ultimately we have eight large national security cutters. The budget between 2011 and 2012 fully funds cutter number 5. We do not provide in the 2012 budget what is called long lead funding for number 6. We have instead a commitment—I think it is actually in writing—by OMB that we will fund number 6, but those funds will not be spent until fiscal year 2013. So we did not park them in fiscal year 2012. We did not think that was an efficient use of them.

So we fully expect to build out the eight cutters. In exchange for not funding lead time for number 6 in 2012, we buy a combination of 46 smaller vessels, fast response cutters and so forth, that could be used in other missions for the Coast Guard and for their lay-down. And then there is some funding in there for aircraft, but those are not made in Mississippi.

DISASTER RELIEF FUND

Senator COCHRAN. Are you satisfied with the request being submitted to the Congress for funding that the FEMA disaster relief fund will have money to respond to emergencies that occur? We think of the hurricanes that hit the Gulf of Mexico, the oil spill that occurred down there. We have had some really serious challenges in that part of the country. What about that disaster fund? Do we have enough money requested in here to meet your needs?

Secretary NAPOLITANO. The disaster fund request for 2012 is based on the historical practice which is to take a 5-year average of noncatastrophic disasters and roll that forward as the number and then rely on a supplemental for catastrophic disasters. So the fiscal year 2012 budget would cover that practice.

As the chair noted earlier this morning, we do have some costs that will necessitate a supplemental. We have been deobligating money. We have been repaying money into the DRF. So what the amount of that supplemental ultimately will need to be I cannot tell you right now.

Senator COCHRAN. Madam Chairman, I think I will reserve the balance of my time.

Senator LANDRIEU. Thank you, Senator.

Senator Lautenberg.

Senator LAUTENBERG. Thank you, Madam Chairman.

Madam Secretary, I talk to you now as the vice chairman of this subcommittee, and I am happy to serve in that capacity.

You have unique experience. You have been on the front lines in terms of your past service as Governor and know how important security, law enforcement is.

FUNDING CUTS

We face urgent threats to our homeland security. It comes from our friends in the House who want to cut funding for programs at the Department of Homeland Security to keep us safe. While the Republicans want to make unreasonable cuts to Government, the fact of the matter is when it hits people's lives, it makes a huge difference, and their plan would slash funding for valuable Homeland Security grant programs like port security, public transportation security by 66 percent. These funds go to our States, cities, and towns. They are the front lines of protecting our homeland. Cuts to these two programs alone would mean approximately \$60 million in Homeland Security support would vanish in my State of New Jersey.

And New Jersey is home to what law enforcement has identified as the country's most at-risk 2-mile area for terrorists, the stretch between the Port of Newark and the National Liberty Airport. It is a region that has contact with 12 million persons, and it is irresponsible to take vital resources away from our most threatened area.

Now, President Obama and you, Madam Secretary, recognize this, and the administration's request takes a more thoughtful approach to funding the Department of Homeland Security. The budget recommends slight increases for urban area security initiatives, State Homeland Security grant programs. These provide vital

support to keep our residents safe. But the budget request level for funding port security and a slight decrease for rail transit and bus security accompanies the fact that the Coast Guard, one of our most valuable resources in our need to protect ourselves, also continues to be asked to do more with less. And we have got to provide the Coast Guard with the resources it needs to effectively handle its many missions.

Although I have some concerns about the request I am going to address in my questions, it will go to you in writing. We are very much out of time. We will go as far as we can right now, however.

This is not a time to cut back on our homeland security. We have seen an increased risk of homegrown terrorism, the Fort Hood massacre, the Time Square bombing attempt, and the New York City subway plot, which was uncovered by our law enforcement people. Incidents like this remind us that the threat of terrorism is as real as ever and we are doing more than skimping on public safety. Are we simply cutting resources or are we cutting the throats of the people in our society?

So, Madam Secretary, I ask how we can continue our work to make vital investments in homeland security.

We talked about the bag charges and what burdens that imposes on the screening process. I look at Newark Airport, one of the largest in the country, and there have been six security breaches at Newark Airport in the last couple of months. Now, I understand that TSA is almost 70 employees short of its allocated number for Newark Airport. What is DHS doing to fully staff Newark Airport and give transportation security officers and managers the training they need?

Secretary NAPOLITANO. Well, I will respond in writing to the specific question on Newark Airport.

[The information follows:]

In close coordination with the Federal Security Director and staff at Newark Airport (EWR), the Transportation Security Administration (TSA) has initiated a robust and multi-layered effort to address EWR staffing vacancies. EWR is currently scheduled to reach near-100 percent staffing by May 1, and, in the interim, TSA has been providing additional resources as needed. For example, TSA deployed additional supervisory training instructors to train new hires, additional AIT-certified Transportation Security officers (TSOs) to conduct daily operations while EWR TSOs are being trained, and additional staff resources to assist in Human Resources and Training operations.

Following a breach, a complete review of the incident is conducted and each action is broken down in detail to ascertain the reasons behind the breach. Every TSA individual involved in the activity and their response is included in this review. TSA employees identified as not having followed standard operating procedures or whose actions are the result of inattention to duty are immediately removed from their position, and can only return to their positions if retraining and recertification for their positions is determined sufficient and is satisfactorily accomplished.

Secretary NAPOLITANO. But, Senator Lautenberg, I think that the President's budget request was designed to meet the threats as we see the threats. One of the things we ask for in there to achieve an efficiency is combining or consolidating grant programs. We have 17 grant programs. We would like to consolidate that significantly to reduce overhead to the grantees, as well as to the grantor. That was something we asked for last year. We did not achieve it, but it is a suggestion that we make to the subcommittee as one area where we could possibly achieve some savings and yet oper-

ationally make sure that we are getting money to where it is needed.

Senator LAUTENBERG. Well, that is a big stretch. Having to do more with less is something we have gotten accustomed to here in these years of difficulty. But we also have to recognize that there are some minimum resources that we have to have to assure the public that we are taking care of their safety.

The House Republicans have proposed cutting port security by two-thirds—the grants. The Port of New York/New Jersey, the largest port on the east coast, the second-largest port in the country, directly linked to what the FBI deemed the most dangerous area in America for terrorist attack, and yet we lose \$33 million in security funding under the House bill. What would be the impact on the New Jersey and New York region on our Nation's economy if there was to be a terrorist attack on one of our largest ports? It is almost unimaginable. The financial center of the world is included in that circumference, as I mentioned before, 12 million people, a large presence of chemical manufacturing in this area, very, very dangerous to the surrounding population. And what are we doing about that? How can we assure the public that they are being well protected, Madam Secretary?

Because time is precious and fleeting here, I will take an answer in writing, and I will have a couple of other questions that I will submit to you and ask for a prompt response, please.

Secretary NAPOLITANO. Senator, all I can say about the House budget for fiscal year 2011 is that it is not a good budget for security. It will have impacts on things like protecting the critical infrastructure along that mile in New Jersey through reductions in grants, through reductions in our personnel. And if that budget becomes the basis for the fiscal year 2012 budget, then I think the Congress needs to understand—and I think my job is to help it understand—that that in all likelihood will have a security impact.

Senator LAUTENBERG. Thank you.

Senator LANDRIEU. Thank you, Madam Secretary.

Senator MORAN.

Senator MORAN. Chairperson Landrieu, thank you very much for the opportunity to join you and Mr. Coats and other members of the subcommittee.

Secretary Napolitano, thank you for your testimony. I look forward to being a responsible and diligent member of this subcommittee and the Appropriations Committee, and I am honored to be here today.

NATIONAL BIO- AND AGRO-DEFENSE FACILITY (NBAF)

In the short time that I have, I wanted to highlight one of the things that is included in your budget that I am very supportive of and want to give you the chance to comment on. You mentioned in your written, as well as your verbal testimony about the National Bio- and Agro-Defense Facility. It is my understanding that the request was initially for \$200 million, now in your budget, having been scrubbed by OMB, at \$150 million. And I would like to express my support and willingness to work with you to see that that is accomplished.

I represent a State in which we are often thought of as the Wheat State, and we are clearly that. But we are very much a livestock, particularly a cattle, State, and we have genuine concern recognized by the Department of Homeland Security about the possibility of animal diseases. Whether they are naturally occurring, accidental, or intentional, they have a dramatic impact upon the economy of Kansas and certainly the country.

We have a very aging facility located on Plum Island that your Department, through a selection process, has concluded a site. In fact, I was there at the announcement in December 2008 about the site for this new facility. And I want to make certain that this Congress and this administration finally fulfill the next step toward building that facility for the safety and security of the American consumer and citizen in light of the risk that we face in this country.

So I just would like to have you reiterate the Department's position, your position, express to the Congress the value of this facility, and how important the timing is for its completion.

Secretary NAPOLITANO. Well, Senator Moran, first of all, the NBAF is something that we are very supportive of. In fact, I saw Governor Brownback Sunday evening and we talked about it and our support for this again.

I would note, however, for you that the House continuing resolution for fiscal year 2011—the part of our Department that is hit the hardest in that resolution is the Science and Technology Directorate. That is where NBAF is located in our budget. It is reduced by half in that House continuing resolution. That is also where we are doing research on new breathing apparatuses for firefighters and research with our national labs on an airport checkpoint of the future, you know, trying to design something so that people do not have to take off their shoes and limit the amount of liquid they can carry on, that sort of thing. But the NBAF is in there as well.

We are very supportive. Plum Island does not meet the Nation's needs in this area. Kansas was the winner of a very highly contested peer-reviewed competition, and we look forward to its continued construction in Kansas. But I must share with you that things are at risk based on the House budget.

Senator MORAN. I would respond, Madam Secretary, that a piece of good news in the debate on the House floor in discussing H.R. 1, the amendment was made to provide that no funding be authorized for this project, and that amendment was defeated. So I was pleased to see the support by a majority of House Members for this project.

I also would add that the State of Kansas has already committed dollars, has already expended resources, and I would guess that there is a bit of reluctance on our part to continue the funding. We have committed \$140 million toward the completion of this project, and we would have—I cannot speak for Senator Brownback, but I know that there would be reticence on the part of many in Kansas in continuing to fund this project in the absence of the Federal commitment. We are anxious for the day in which the first shovelful of dirt—we would love to have you there and join us with the shovels that begin the Federal commitment on that day.

Secretary NAPOLITANO. And, Senator, I think we share that commitment. We believe in the NBAF, and it should be in Kansas, and we need to get on with it.

Senator MORAN. I appreciate those sentiments and I thank the chairperson for allowing me to have this conversation.

COAST GUARD CUTS

Senator LANDRIEU. Thank you, Senator.

Madam Secretary, the Department of Defense budget this year is being increased by \$23 billion, a 4-percent increase, and that is excluding the cost of the wars in Iraq and Afghanistan.

The Coast Guard's discretionary budget has increased less than 1 percent. The Coast Guard is one of the five armed forces of the United States. Some of us are having difficulty understanding how it can be treated almost as a stepchild given the work that it is asked to do in direct protection of our Nation, whether it is intercepting drugs, responding to disasters, responding to catastrophic oil pollution incidents, which just occurred.

Can you shed any light as to why the sixth security cutter was deferred? I mean, I understand we have budget constraints but could you comment just about the importance of maintaining the Coast Guard operations for the security of our Nation?

Secretary NAPOLITANO. Well, Senator, the sixth security cutter was not deferred in the sense of unnecessarily delayed, but the plain fact of the matter is that by the time we actually need to expend money for six, given the time it will take to finish four and five, we will be into fiscal year 2013. And our plan is rather than set aside unusable money for six in fiscal year 2012, that we would request the amount in the year we needed to expend it, which would be fiscal year 2013.

Senator LANDRIEU. Okay. Well, let us continue to focus on that.

GULF COAST DUMPING

Another issue that is of particular interest—and I hate to be so parochial because I do have my eyes on the whole country. But right now along the gulf coast, we are having such serious issues, you know, with the moratorium, the gulf coast spill, still recovering from Katrina and Rita, and this is the whole gulf coast from Florida to Texas.

But another issue—and it may be affecting some of the other coastal States as well—is the illegal dumping of seafood wrecking our domestic markets. We are having a terrible time in this area. Customs in my view is simply not doing enough to collect the dumping duties that importers owe to the Federal Government. Since 2005, for example, importers of shrimp from China have failed to pay more than \$58 million in dumping duties.

So, Senator Coats, when we are looking for some additional funding, we could be more efficiently collecting some of the money that China or Vietnam or others owe us, using that money to invest or support or give, if not rebates—according to WTO, that may be inappropriate—but in some way capturing those funds.

So could you comment on what is in your budget to enforce these antidumping rules and regulations on that subject?

Secretary NAPOLITANO. Well, I think it would be better if we addressed those in writing for you. I know there was some concern. I believe there is a rule on crawfish, if I am not mistaken, among other types of seafood. I would like to discuss with my component heads what the problem is, if there is a problem, and come back to you with a detailed answer.

[The information follows:]

Antidumping/Countervailing Duty (AD/CVD) Enforcement is a priority trade issue (PTI) for Customs and Border Protection (CBP). CBP takes a concerted, systematic approach to detect and deter circumvention of the AD/CVD law, administer entries of AD/CVD merchandise, and to issue and collect bills for AD/CVD duties owed to the United States Government. CBP coordinates its AD/CVD enforcement activities through an intra-office AD/CVD PTI Working Group. CBP works closely with the U.S. Department of Commerce (Commerce), the administering authority for AD/CVD determinations under U.S. law, and U.S. Immigration and Customs Enforcement to enforce AD/CVD laws and regulations.

When CBP issues a bill for final AD/CVD duties, CBP makes every effort to collect all duties, taxes and fees legally due to the Government. However, some importers, or their agents, are unable to pay the final duties. In addition, at least two sureties issuing bonds covering substantial amounts of AD/CVD duties are currently in receivership, further complicating collection. Other importers are simply unwilling to pay, or no longer exist by the time CBP issues a bill. CBP pursues collection action against importers and sureties who are simply unwilling to pay. CBP's Revenue Division in the Office of Administration initiates an administrative collections process in order to recover past-due amounts from the importers and sureties. This process may include dunning letters and the suspension of the immediate delivery process, among other steps. Ultimately, those debts for which the Revenue Division's collections process is ineffective are referred to CBP's Office of Chief Counsel.

The Office of Chief Counsel pursues collection from both the importers and sureties, after completing a legal review of the underlying debt. Further, a review is done to determine if there is a viable importer (or available surety coverage) from which the debt may be recovered. In part, this is done through dunning letters, searches of electronic databases and internal systems, and pursuing available leads. In addition, CBP can assess civil penalties pursuant to 19 U.S.C. § 1592 against any party who, by fraud, gross negligence, or negligence submits a material false statement or omission on importation into the United States, including those cases in which a false statement or omission is made concerning the applicability of an antidumping duty order to a particular entry. If administrative attempts to collect the debt are unsuccessful and a viable importer and/or surety can be found, the Office of Chief Counsel drafts a complaint and refers the matter to the Department of Justice for possible litigation in the Court of International Trade. If the Office of Chief Counsel is not successful in locating a viable entity to be pursued, the matter will be referred back to the Revenue Division for appropriate action. This may include referral to Immigration and Customs Enforcement for further investigation. If the debt is without legal merit or no viable entity can be located to pursue further collection action, CBP may ultimately be forced to write off the debt.

CBP has taken steps to specifically improve the collection of AD/CVD duties on shrimp imports and continues to explore statutory and nonstatutory changes to enhance bonding requirements. CBP is also actively pursuing collection of the balance of the open bills against delinquent importers and sureties.

Senator LANDRIEU. Thank you.

And I want to submit for the record—then I will turn it over to Senator Coats. I think he may have another question or two. Senator Murkowski has joined us—but for the record about the DRF. I asked the staff to provide—and I am going to submit for the record—a 20-year history of emergency supplemental funding. Out of the \$128 billion that has been allocated by the Federal Government for emergency response to all sorts of disasters, \$110 billion has been appropriated through the supplemental process. So \$110 billion out of \$128 billion.

And when you look at this list, you can understand why that occurs because these sums range from a low of \$143 million budgeted

one year to \$50 billion another year. So there are wild fluctuations and very difficult to predict what is going to happen. And as Senator Coats and I were saying, these storms seem to be getting more frequent, flooding more frequent, levels of flooding higher, more aggressive kind of storms and weather patterns.

So I submit this for the record because I actually think this subcommittee is going to have to push hard to get this emergency funding in a supplemental and use the base funding of Homeland Security to manage the operations of this important function of Government. So if I can have unanimous consent to submit that to the record.

[The information follows:]

DISASTER RELIEF NONEMERGENCY/EMERGENCY HISTORY

Fiscal year	Public Law	Annual or supp	Amount	
			Nonemergency	Emergency
1992	102-139	Annual	\$185,000,000
1992	102-229	Supp	800,000,000	\$143,000,000
1992	102-302	Supp	300,000,000
1992	102-368	Supp	2,893,000,000
1993	102-389	Annual	292,095,000
1993	103-75	Supp	2,000,000,000
1994	103-124	Annual	292,000,000
1994	103-211	Supp	4,709,000,000
1995	103-327	Annual	320,000,000
1995	104-19	Supp	3,275,000,000
1996	104-134	Annual	222,000,000
1996	104-19	Supp	3,275,000,000
1996	104-134	Annual (rescission)	(1,000,000,000)
1997	104-204	Annual	1,320,000,000
1997	105-18	Supp	3,300,000,000
1998	105-65	Annual	320,000,000
1998	105-174	Supp	1,600,000,000
1999	105-276	Annual	307,745,000
1999	105-277	Supp	906,000,000
1999	106-31	Supp	900,000,000
2000	106-74	Annual	300,000,000
2000	106-74	Supp	2,480,425,000
2001	106-377 (H.R. 5482)	Annual	300,000,000	1,300,000,000
2001	107-38 ¹	Supp	1,791,000,000
2002	107-73	Annual	664,000,000	1,500,000,000
2002	107-117 ²	Supp	4,356,871,000
2002	107-206	Supp	2,650,700,000
2002	107-206	Supp	23,200,000
2003	108-7	Annual	800,000,000
2003	108-69	Supp	983,600,000
2004	108-90	Annual	1,800,000,000
2004	108-83	Supp	441,700,000
2004	108-106	Supp	500,000,000
2004	108-303	Supp	2,000,000,000
2005	108-334	Annual	2,042,380,000
2005	108-324	Supp	6,500,000,000
2005	109-61	Supp	10,000,000,000
2005	109-62	Supp	50,000,000,000
2005	109-148	Supp (rescission)	(23,409,300,000)
2006	109-90	Annual	1,770,000,000
2006	109-234	Supp	6,000,000,000
2007	109-295	Annual	1,500,000,000
2007	110-28	Supp	3,400,000,000
2007	110-28	Supp	710,000,000
2008	110-161	Annual	1,400,000,000
2008	110-116	Supp	2,900,000,000

DISASTER RELIEF NONEMERGENCY/EMERGENCY HISTORY—Continued

Fiscal year	Public Law	Annual or supp	Amount	
			Nonemergency	Emergency
2008	110-252	Supp	897,000,000
2008	110-329	Supp	7,960,000,000
2009	110-329	Annual	1,400,000,000
2010	111-83	Annual	1,600,000,000
2010	111-212	Supp	5,100,000,000
Total	17,635,220,000	110,386,196,000

¹ Amount provided by FEMA law is not specific by Agency.

² From amounts appropriated but not originally specified in Public Law 107-38.

Senator LANDRIEU. Let me recognize Senator Coats for a second round, then Senator Murkowski, and then Senator Moran.

Senator COATS. Madam Chairman, thank you. Just one question and then I will submit some questions also for you to respond back.

Senator LANDRIEU. And then we are going to have a break in about 5 minutes to——

Secretary NAPOLITANO. I will try to keep my answers short.

Senator COATS. I will try to keep my question short.

STATE AND LOCAL COMMUNITIES, GRANTS

Looking at the grants to States and local communities, I think the total in the budget request is \$3.8 billion, which is about 9 percent of the Department's total discretionary request. That will be in addition to \$28 billion, as I understand it, that has been appropriated since fiscal year 2004.

The question is, it is my understanding that we have not really been able to fully assess—although FEMA is undertaking something to this effect—how effective these are and particularly whether the distribution of these funds is appropriate. The problem usually arises on grants and distributions as the political animal raises its head and basically says I got to get my share.

So I am sympathetic to what Senator Lautenberg was saying relative to representing an area that is a significantly high-threat area with the consequences being very, very significant. That obviously is going to be a more significant and higher priority area than several of my rural towns or Jersey's rural towns.

But if we keep insisting on a revenue-sharing program in which everybody gets a slice, it may be that given this fairly extraordinary amount of money that has been spent to upgrade and prepare local responders and so forth needs to be triaged in a more effective way.

Now, I say that meaning that there may be some communities in Indiana that might not get what they otherwise would have gotten in deference to the fact that we have identified some more-highly targeted, more-significant consequences if we have an attack here or in a particular area and so forth.

Could you comment on that in terms of, one, how we best assess the impact and the effectiveness of that \$28 billion that has already been spent and whether or not we need to make an effort at looking at prioritizing or triaging areas which ought to get more funds and others that should get less?

Senator LANDRIEU. Let me interrupt just 1 minute. In the spirit of bipartisanship, I am actually going to pass the gavel to Senator Coats so he can continue. I am going to go vote and in 5 minutes you all could take a recess, and then I will be right back. But you all continue.

Senator COATS [presiding]. All right.

Secretary NAPOLITANO. I am glad because this requires a longer answer I think than perhaps the buzzer would permit.

In the area of grants, one of the things we need to do as a country is—I call it a homeland security architecture that begins with small towns, cities, States, et cetera. The Federal Government cannot do it by itself. And I think the theory underlying a lot of the grants is that being the case, we need to make sure that there is a certain baseline capability throughout the country.

And then second, in the area of focusing Federal grants on the areas of highest risk, there I think there needs to be and can be and should be a dialogue with the executive branch and the legislative branch. I will share with you, Senator, that one person's rural community is another person's—subject to an ag or a bio-attack and the need to have things like the NBAF located there.

So on the issue of interoperability of emergency response equipment, rural America is the toughest problem. In urban areas, interoperability can be achieved and is being achieved because the lines are there, the towers are there, and so forth. In rural America or the area along the Southwest Border or along the Northern Border, it is some of our most difficult areas to cover just because of the lack of capital and infrastructure. So these are kind of the nuts and bolts things we are going through when we talk about awarding grants for interoperability or for this or for that.

But I think you are right to suggest that there can be a useful dialogue on how grants are done. That is why we have recommended that some of these programs be consolidated because we think that that would be a better way to manage them and so forth. So we look forward to working with the subcommittee on that.

Senator COATS. Thank you.

Senator Murkowski.

Senator MURKOWSKI. Thank you, Senator Coats.

Secretary, welcome. I apologize I was not here for the full hearing. I will make my comments quick, hopefully, and will get out of here to the vote. And I do not know whether you have to stay until we get back or not. But let me go very, very quickly.

TSA PAT-DOWNS

I was up in Alaska this past weekend, and all of the news was centered around one of our State House Representatives, Representative Sharon Cissna, a woman that I have served with, a woman who has undergone breast cancer and had a mastectomy. And you do not need to know her personal history, but her personal history is now part of the discussion in Alaska because she was subjected to what she felt was a very intrusive pat-down coming back from Seattle to go to work in Juneau after her medical appointments. And apparently the full-body scanners detected some scars, and apparently Representative Cissna is not the only indi-

vidual where scars from medical procedures are picked up and the individual is subjected to what is described as a very intrusive pat-down.

She had made the determination that she was not going to put herself through this again. She had done it once. And as a consequence, this individual, in order to get back to work, drove a car, took a small airplane, went through Canada, and eventually got onto the ferry. It took her 4 days to get from Seattle to Juneau. Our State's capital is on an island in Alaska. We cannot get anywhere without flying.

I have sent a letter to the Administrator of the TSA asking him for clarification as to what the process will be for those that have had medical procedures, those that have prosthetics that go through this screening process where they are subjected to enhanced pat-downs and the intrusion on their dignity is such that they are making choices like Representative Cissna did to not fly. In my State, as you know, that is a pretty difficult decision to make.

I have not heard anything back from the Administrator about this yet, but it is an issue that as we work to protect the safety of all Americans and the safety of our skies, the safety of our Nation, there is that balancing between how we ensure for that and how we ensure for an individual's privacy and dignity.

I wanted to make sure that you were fully aware of this because this is an issue that has taken on a life beyond its own. And I do not know whether you have an answer for me today in terms of what those protocols may be, but it is something that I believe the issue will not die down until there is a better resolve than what we saw happen, at least with one particular constituent in the Seattle airport.

Senator COATS. Madam Secretary, if I could, just in the interest of time here, I am going to pass the gavel to my colleague and let you answer her. I think by the time Senator Murkowski is done, the chairman will be back. I just got a note she is returning. So if there is a little break, we will just take a temporary recess.

Secretary NAPOLITANO. Fair enough.

Senator MURKOWSKI [presiding]. Thank you.

Secretary NAPOLITANO. I can chair the subcommittee if you want. Just kidding.

All right. First of all, Senator, we will look into this particular matter. It strikes me as a highly unique one, but we will—

Senator MURKOWSKI. I am told it is not and that is why—

Secretary NAPOLITANO. Well, we will find out.

Senator MURKOWSKI [continuing]. So I think it is important.

Secretary NAPOLITANO. We will find out—

Senator MURKOWSKI. Good.

Secretary NAPOLITANO [continuing]. Because I will share with you that this is not designed to be invasive in the sense of unnecessary or a harassment of any sort. And we want to make sure we work through this particular issue. So we will do that.

I will also share with you, however, that overall we are finding that the AIT process, which is the new technology we are using—99.9 percent of the passengers who have been through it since Thanksgiving have gone through it, no opt-outs, no anything. Peo-

ple with artificial joints, artificial hips, for example, love it because it can clearly distinguish that versus the magnetometer where they always were getting pulled aside.

The particular issue you raised—this is something that I am more than prepared to look into. We will provide you with a response. No one with a medical condition should feel like every time they have to go through the screener, they are going to get pulled aside because of their medical condition. What we want to pull aside are individuals for whom we cannot resolve an anomaly on the screen. This is our last line of protection for an aircraft. There are a lot of things that go on before you get to that point, but that is our last line. So we will get back to you on that.

[The information follows:]

TSA SCREENING PROCESS FOR PERSONS WHO HAVE HAD MEDICAL PROCEDURES

TSA spoke with Senator Murkowski's staff and discussed TSA's working relationships with groups like Susan G. Komen foundation to address issues raised by Alaska Representative Cissna for women who've undergone mastectomies and how TSA integrates their suggestions into training. Also shared were TSA's conference calls and other outreach with Representative Cissna about her experience. The following summarizes this information:

Does scarring from a mastectomy regularly cause an AIT alarm?

There are many possible factors that may generate anomalies during Advanced Imaging Technology (AIT) screening, including breast prosthetics or surgical scarring.

When an anomaly is discovered during AIT screening, the Transportation Security Officer (TSO) must resolve the alarm using additional screening procedures. TSA's procedures do not require that passengers remove their breast prosthesis as part of the security screening process. If a pat-down is required to resolve the anomaly, it may be done in a private screening area and will be performed by an officer of the same gender. A TSA witness will be present if the pat-down is conducted in the private screening area. The passenger may have a witness of their choosing accompany them throughout the screening process regardless of whether the screening occurs in the public or a private screening area.

What training do TSO's receive related to this issue?

TSOs are instructed, as part of their training and standard operating procedures, to use extreme care and sensitivity when screening or performing pat-downs of sensitive or painful areas. We also urge travelers to tell TSOs about any specific issues TSOs should be aware of before such screening measures begin, including painful or sore areas, or past and current medical conditions. To ensure the greatest level of privacy possible while conveying sensitive information, TSA has also made a notification template available for passengers to discreetly provide information about their medical condition or disability to TSOs at airports. The template is available at TSA.gov and TSA has proactively shared it with a coalition of 70 advocacy groups representing a variety of segments of the population with whom TSA maintains an ongoing dialogue. A number of cancer-related groups have been a part of the coalition, including Susan G. Komen and Cancer Treatment Centers of America. Based on input we received from groups such as these over the last year, we have augmented the training provided to our TSOs to make them better attuned to the needs of cancer survivors and those who have recently undergone cancer treatment.

Senator MURKOWSKI. And I appreciate you looking into that. The Alaska State legislature—excuse me—the House of Representatives has passed a resolution in support of Representative Cissna's effort to get some clarification to the process. I will forward all of this to you and look forward to working with you, sharing some of the information that I have raised.

COAST GUARD ICEBREAKERS

Very quickly then a second question, and then I will submit a third for the record. This is as it relates to our Coast Guard to our

ability to respond in an ever-growing Arctic. I was pleased to see that the fiscal year 2012 budget restored the funding for the operational control for our icebreaker fleet to the Coast Guard. I think that that makes sense. That is important.

But contained within that budget is the decommissioning of the *Polar Sea* in fiscal year 2011. It provides for completion for the maintenance of the *Polar Star*, but that will not be complete until 2013. So we have got a situation here where at least for the next couple years we have the *Healy* out there in the waters, but we do not have any polar class icebreakers, and it leaves us without the capacity to do any heavy icebreaking capability until then.

So the question to you is with the fact that the Coast Guard will only have one heavy icebreaker once the *Polar Sea* is down and the *Polar Star* is up, what are the Department's plans? What are the Coast Guard's plans for the future of this country's heavy icebreaking fleet? If you can give me the status of the Coast Guard's high-latitude study and when you might expect that that might be available for release to us here in the Congress.

Secretary NAPOLITANO. Indeed. First of all, my understanding is the *Healy*, which is a medium-sized cutter, will remain operational in 2011–2012. The problem is you have the *Polar Star* and the *Polar Sea*, both of which are old vessels and need to have heavy maintenance. And so you have this—it looks like a bare period in fiscal year 2012.

Our plan is during that period for the National Science Foundation to lease a heavy icebreaker to take the place—

Senator MURKOWSKI. Who do we lease from?

Secretary NAPOLITANO. There are at least two countries that we can lease from. I would prefer to give that to you in writing—or not in writing, but not in an open session. But we have identified at least two countries that we could lease from during that fiscal year 2012 period.

[The information follows:]

The National Science Foundation (NSF) has leased polar icebreakers from both Russia and Sweden in the past. NSF is continuing to negotiate their specific polar icebreaking requirements lease plans for 2012 and the details of that lease should be directed to NSF.

Secretary NAPOLITANO. Now, as you said in your question, you got the funding for operational control up there, \$39 million moved over to the Coast Guard. That is where it should go.

We also have in the fiscal year 2012 budget a sum set aside for an Arctic study. One of the things this country really needs is to really look at the Arctic and what is necessary to protect U.S. interests there. So that is in the Coast Guard budget as well.

With respect to the work—you wanted to know when the other study would be finished. Let me check with the Commandant and we will get you the date.

Senator MURKOWSKI. I appreciate that.

And I appreciate the information on what we do to fill the gap here with the heavy icebreaker. I do hope that we are not moving in a direction where we view that as our option to lease basically commercially. I think we need to remember that we are an Arctic nation. The United States is an Arctic nation, and the fact that we have just barely one-and-a-half icebreakers, if you will, when you

think about the medium and the heavy, it is a situation where we look to our ability to respond as an Arctic nation whether it is the level of shipping traffic that we are seeing going on up north, the level of exploration activity that may be at hand. We have got cruise ships going back and forth up in the Arctic right now. We are woefully unprepared, I believe, at this point in time. So I would love to discuss kind of the future of where we go and how we build this out so that we are able to respond as necessary. But again, we are behaving as an Arctic nation and assuming that international role that I think that we should as a Nation.

Secretary NAPOLITANO. I could not agree more.

Senator MURKOWSKI. Thank you, Madam Secretary.

And I guess we are at ease until Senator Landrieu comes back.

Secretary NAPOLITANO. Thank you, Senator.

Senator LANDRIEU [presiding]. Our meeting will come back to order after a brief recess, Homeland Security Subcommittee Appropriations meeting.

GOVERNMENT SHUTDOWN

Let me begin with just another question about the potential—and I hope we can avoid this, Madam Secretary, but the potential shutdown of the Government and what that might mean for the Department of Homeland Security. The Government was shut down for 27 days in 1995 and 1996. The front-line personnel for Customs Service, Border Patrol, and Secret Service continued to work, but their workers were not immediately paid. I understand their support operations or administrative operations did not continue to work. So you have to question how effective their work can be without any back-office support.

But if the Government were to shut down again—and again, we are all working hard to see that that does not happen and coming to some compromise with the House on this—what would be the impacts to the Department? I am sure you have given some thought to this.

Secretary NAPOLITANO. Thank you, Madam Chair. Yes, I have in part because this Department did not exist in 1995 during the prior shut-downs, and so we have had to be looking at this afresh, anew because the Department is only 8 years old.

Thank you again, by the way, for coming to the program yesterday. It was really great to see you there.

I think you put your finger on one of the important points. The front-line personnel who are related to security would fall within the exception of the shutdown and they would stay on duty, but the back-room personnel that are necessary to fully utilize the front-line personnel would not in all likelihood. And our TSOs, our transportation security officers, our front-line personnel, tend to be at the lower end of the pay scale and tend to be ones that I would be very concerned about having to live paycheck-to-paycheck. And so you would have your front-line personnel who were working but not getting paid and being under some financial duress because of that. So we have parts of the Department that would probably have to shut down virtually 100 percent, but the security-related part would operate, but as you say, they would not have the full backing of the Department that they would otherwise have.

Senator LANDRIEU. Thank you. I do think that is something that we need to keep in mind as we press forward on these negotiations.

OFFICER CORRUPTION

My next question—I only have three additional questions, and I think we can get through them in the next few minutes—is about the officer integrity, the issue of integrity in our operations. I think not only in trying to streamline where we can is important without undercutting our defense and homeland security, but also we want to have an honest and open and transparent Government, which is always so important. And of course, America is really a model in the world. We are proud of that. We are not perfect, but we are a model in that regard.

But there have been some concerns that this subcommittee has expressed, and I want to just state that with the support of this subcommittee, U.S. Customs and Border Protection has hired 16,000 new employees, a 37-percent increase in the last 5 years. U.S. Immigration and Customs has hired more than 8,200 new personnel. This has been required to stand up this Department and meet the goals and objectives of securing our borders and enforcing our immigration laws.

This subcommittee has been concerned, however, due to the rapid hiring, that there is a potential increase for officer corruption. So towards this end, the subcommittee has provided additional resources for integrity training, investigations, conducting hearings about misconduct, background investigations. I am pleased to see your budget requests an additional \$26 million for this. This is the right thing to do. I support the funding.

But it is our understanding that some of the people in charge of this from CBP to ICE and the Inspector General are experiencing some difficulty working together. Could you comment about if you are aware of this situation? Do you agree that it is somewhat of a problem? And if so, what are you doing to correct it? Will you and the Deputy Secretary work with me on establishing clear lines of authority for these important internal investigations?

Secretary NAPOLITANO. Madam Chair, I think that it is fair to say that with that rapid increase, we need to have appropriate oversight and supervision for a number of reasons, one of which is related to officer integrity. And so we have ramped up efforts there.

I think it is also accurate to say that we have been working both with the OIG's Office and with CBP on the implementation of appropriate oversight, what does that mean, who does what when. How do we make sure that cases are resolved swiftly so that agents are not unduly impugned or taken off the line and that if and when we find an agent who has become corrupt, that we deal with that immediately and very firmly? We will not stand for corruption among our troops and we do not want that bad seed to take root in this staffing increase. So we are all very committed to that goal.

The issue is how do you operationalize that between the OIG and what the CBP does and what ICE does, and that is an issue of which I am very aware, have been personally involved in, and we continue to work on.

Senator LANDRIEU. And do you have the money and resources you need for the polygraph and the initial checks before hiring peo-

ple? Are you able to process your hirees pretty quickly, do you believe?

Secretary NAPOLITANO. The President's budget contains adequate resources for that, yes.

MEXICO

Senator LANDRIEU. My next question—and this is a growing concern among, I think, people in our country, and that is the escalating violence in Mexico. You alluded to, of course, we lost one of our special agents, Zapata, just recently and another was wounded. This really brought to light the fact that our agents are prohibited from carrying service weapons in their defense, which is a side issue.

But the more important issue—and that is important as well—is that 33,000 Mexican citizens have died during the Mexican Government's admirable, but very difficult campaign against drug trafficking. But what are the top one, two, or three directives that you are taking to try to contain this violence? And when we are sending agents, is it appropriate to send agents into Mexico without being able to defend themselves?

Secretary NAPOLITANO. Well, first of all, I would suggest, Madam Chair, that some of this be discussed in a classified setting and that includes how the agents are armed and under what circumstances.

I will say that the violence in Mexico is something we are very concerned about. It is one of the things that we work on very closely with Mexico. President Calderon is scheduled for a visit to the United States this week. I believe that will be something that he and President Obama discuss. And it is something that we are working with Mexico on.

Some of our priorities are to assist Mexico in any way that we can and as requested to defeat the cartels.

Number two, to make sure that we have adequate resources along our Southwest Border to prevent the cartels from bringing their violence over and trying to take over areas along the Southwest Border, so preventing spillover violence.

And then number three, making sure that we have adequate manpower, technology, and infrastructure along the Southwest Border as a whole so that it can be a safe and secure zone for the trade and travel that has to occur between Mexico and the United States. This is something that often gets overlooked in the discussion, but Mexico is the number one or two trading partner of something like 23 States in the United States. There are a lot of jobs associated with that commerce with Mexico. So both countries need to work to make sure that the travel and trade that occurs can go smoothly and efficiently through the ports of entry.

Senator LANDRIEU. Thank you.

CYBER THREAT

I think my last question will be about the cyber threat, which is something that I am not sure that the public really sees. I think they see and read about the violence in Mexico. I think they understand some of the border issues. I think they understand the challenges of immigration. I think they most certainly can understand

the airline attacks and the New York incident. But cyber is something that I am not sure the public really can understand the consequences, really, of such an attack, should it occur in a more successful way because we are actually being attacked through this new method.

So my question is, President Obama said that cyber threat is one of the most serious economic and national security challenges that we face. I actually agree with that. You included safeguarding and securing cyberspace as one of the five missions. This budget request appears to respond to this alarm by requesting a robust level of funding for U.S. operations, Federal network, security network, and security deployment. These are important areas. I was pleased to see some of the upticks that you have.

As you know, there are several locations around the country that are really leaning toward actually working in conjunction with non-Federal partners. Corporations have really stepped up. The National Guard has shown an inclination to put some resources towards this.

We have created in Louisiana—in Shreveport, in Bossier Parish to be exact, in the northwest corner of Louisiana—the Cyber Innovation Center. The center has built a strong regional network among universities and colleges to leverage cybersecurity systems.

I would like to ask you for a general comment about the cyber threat and then ask you if you would join me for a trip there and to perhaps a few other locations around the country to see what some of the new initiatives are to actually stand up the technology and personnel necessary to respond to this very serious and I think underestimated threat to our country.

Secretary NAPOLITANO. Madam Chair, yes, we have increased our cyber budget. Between DHS and the Department of Defense, you really have between those two Departments 95 percent of the cybersecurity responsibilities identified by the President's cyber review. So you have seen that area of DHS expand fairly dramatically over the last 2 years. This is another area where we believe that the United States has real security interests involved. We are working with the private sector on this. We also are working with the universities on this, and we are increasing our outreach trying to identify persons who have a cyber background to come work at DHS. That is one of our key challenges is to get enough personnel who are cyber-experienced to work in the public service as opposed to the private sector. So that is underway as well.

With respect to your invitation to come to Shreveport and to do some other cyber site visits, I would be happy to do so, particularly if there is a good Louisiana meal involved.

Senator LANDRIEU. Thank you, Madam Secretary. I think we can rustle one up for you.

Secretary NAPOLITANO. There you go.

CLOSING

Senator LANDRIEU. I am going to end the meeting, but I do want to comment that there are a few other issues that our subcommittee is going to be focused on.

The TSA screener cap provision at 46,000. I do not know if that is going to be effective.

International adoptions is an important issue to me to make sure that we are doing the very best we can in customs to support the great work that our nonprofits and individual citizens are doing in that humanitarian area.

Improving the entry process for visitors to the United States I think is important, whether they are just tourists or whether they are business people traveling because of just the economy of the world, and we have just got to be a very forward-leaning service agency to support that work.

The flood maps are of great concern to myself, Senator Cochran, and other Senators up along the Mississippi River which comes under this subcommittee's jurisdiction.

So those are some questions that I will defer and submit to you in writing.

And I believe that will end our session for today. I thank you for your testimony and for your patience during the floor vote.

ADDITIONAL COMMITTEE QUESTIONS

Senator LANDRIEU. Other questions for the record should be submitted to the subcommittee staff by close of business on Thursday.

[The following questions were not asked at the hearing, but were submitted to the Department for response subsequent to the hearing.]

QUESTIONS SUBMITTED BY SENATOR MARY L. LANDRIEU

DEPARTMENTAL ACQUISITIONS

Question. For each of fiscal year's 2010–2012, how much funding is dedicated to major acquisitions? For each year, provide details on the classification level of each acquisition, i.e. how many are designated as level 1, level 2, or level 3 as defined by the Department's acquisition management directive? Provide a DHS major acquisition status tracking chart listing each program and milestone necessary to achieve approval for full-scale procurement.

Answer.

	Fiscal year 2010	Fiscal year 2011	Fiscal year 2012
Funding dedicated to major acquisitions	\$11,671,000,000	\$11,068,000,000	\$10,457,000,000
Level 1	46 programs	45 programs	Information not yet available.
Level 2	40 programs	37 programs	Information not yet available.
Level 3	Not reported ¹	Not reported ¹	Information not yet available.

¹ In accordance with Directive 102–01 (D 102–01), non-IT level 3 programs are not reported; however, guidance will be changed April 30, 2011, to require inclusion of all level 1, 2, and 3 acquisition programs in the Next Generation Periodic Reporting System (nPRS).

The following chart lists the 82 DHS level 1 and 2 programs along with their current phase in the acquisition life cycle. Programs in phase 4 should be considered approved for “full-scale production”.

The phases as defined in the D 102–01 are:

- Phase 1. Need.
- Phase 2. Analyze/Select.
- Phase 3. Obtain.
- Phase 4. Produce/Deploy/Support.

Please note that the list identifies many programs as being in multiple stages. Typically, these programs are comprised of smaller projects and these projects are in various stages. Accordingly the list identifies such programs as being “mixed” and the lists identifies each stage the program is in.

Program-Project-Service	Phase			
	1	2	3	4
CBP—Advance Passenger Information (API) (P) ¹	x

Program-Project-Service	Phase			
	1	2	3	4
CBP—Automated Commercial Environment (ACE)/International Trade Data System (ITDS) (P)			X	X
CBP—Automated Targeting System (ATS) Maintenance (P)				X
CBP—Border Patrol Facilities (P)			X	X
CBP—Facilities Management and Engineering Tactical Infrastructure (FM&E TI) (P)			X	X
CBP—Fleet Management (FMP) (P)				X
CBP—Land Ports of Entry Modernization (P)			X	X
CBP—Non-Intrusive Inspection (NII) Systems Program (P)			X	X
CBP—SAP (P)				X
CBP—Strategic Air and Marine Plan (P)			X	X
CBP—Tactical Communication (TAC—COM) (P)	X			X
CBP—TECS Modernization (P)			X	X
CBP—Transportation (P)				X
CBP—Western Hemisphere Travel Initiative (WHTI) (P)				X
DHS—A&O—Common Operational Picture (COP) (P)			X	X
DHS—A&O—Homeland Security Information Network (HSIN) (P)			X	X
DHS—CAO—Electronic Records Management System (ERMS) (P)	X			
DHS—CAO—St. Elizabeths (P)			X	
DHS—CFO—Transformation and Systems Consolidation (TASC) (P)		X		
DHS—CHCO—HR—IT (P)			X	X
DHS—CIO—Infrastructure Transformation Program (ITP) (P)			X	X
DNDO—Advanced Spectroscopic Portal (ASP) Program (P)			X	
FEMA—Grants Management Integrated Environment (GMIE) (P)		X		
FEMA—Housing Inspection Services (HIS) (P)			X	X
FEMA—Integrated Public Alert and Warning System (IPAWS) (P)	X			
FEMA—Logistics Supply Chain Management System (LSCMS) (previously TAV) (P)		X		
FEMA—Risk Mapping, Analysis and Planning (Risk Map) (P)				X
A&O—National Security System Program (NSSP) (P)		X		
A&O—Online Tracking Information System (OTIS) ² (S) ³			X	X
ICE—Atlas (P)			X	
ICE—Detention and Removal Operations (DRO) (S)		X		
ICE—Detention and Removal Operations Modernization (DROM) (P)			X	X
ICE—DRO Electronic Health Record (EHR) System (P)	X			
ICE—Enforcement Information Sharing (EIS) (P)	X			
ICE—Student and Exchange Visitor Information System (SEVIS I and II) (P) (SEVIS I=4, SEVIS II=2)		X		X
ICE—Tactical Communication (TAC—COM) (P)			X	
ICE—TECS Modernization (P)		X		
NPPD—Federal Protective Services (S)				X
NPPD—IICV (Infrastructure Information Collection Program and Visualization)—IICP (P)			X	X
NPPD—National Cybersecurity and Protection System (NCPS) (P)			X	X
NPPD—Next Generation Network (NGN) (P)		X	X	
NPPD—United States Visitor and Immigrant Status Indicator Technology (US-VISIT) (P)	X		X	X
OHA—Bio Watch Gen-3 (P)		X		
S&T—National Bio and Agro-Defense Facility (NBAF) (P)		X		
S&T—National Biodefense Analysis and Countermeasures Center (NBACC) Facility (P)			X	
TSA—Electronic Baggage Screening Program (EBSP) (P)			X	X
TSA—Field Real Estate Management (FREM) (P)				X
TSA—HR Access (P)				X
TSA—Information Technology Infrastructure Program (ITIP) (P)				X
TSA—National Explosives Detection Canine Team Program (K9) System (P)				X
TSA—Passenger Screening Program (PSP) (P)			X	X
TSA—Screening Partnership Program (P)				X
TSA—Secure Flight (P)			X	
TSA—Security Technology Integrated Program (STIP) (P)			X	X
TSA—Specialized Training (P)				X
TSA—Transportation Worker Identification Credentialing (TWIC) (P)				X
TSA—TTAC Infrastructure Modernization Program (TIM) (P)		X		
USCG—C4ISR (P)				X
USCG—CG Logistics Information Management System (CG—LIMS) (P)		X		
USCG—Coastal Patrol Boat (P)				X
USCG—Core Accounting System (CAS) (P)				X
USCG—Fast Response Cutter (FRC) (P)			X	
USCG—HC—130H Conversion/Sustainment Projects (P)			X	
USCG—HC—130J Fleet Introduction (P)				X

Program-Project-Service	Phase			
	1	2	3	4
USCG—HC—144A Maritime Patrol Aircraft (MPA) (P)	X
USCG—HH—60 Conversion Projects (P)	X
USCG—HH—65 Conversion/Sustainment Projects (P)	X
USCG—Interagency Operations Centers (IOC) (P)	X
USCG—Medium Endurance Cutter Sustainment (P)	X
USCG—National Security Cutter (NSC) (P)	X
USCG—Nationwide Automatic Identification System (NAIS) (P)	X	X
USCG—Offshore Patrol Cutter (OPC) (P)	X
USCG—Patrol Boats Sustainment (P)	X
USCG—Rescue 21 (P)	X
USCG—Response Boat—Medium (RB-M) (P)	X
USCG—Unmanned Aircraft Systems (UAS) (P)	X
USCIS—Application Support Centers (ASC) (P)	X
USCIS—Benefits Provision—Verification Information System (VIS) (P)	X	X
USCIS—Integration Document Production (IDP) (P)	X
USCIS—Transformation (P)	X
USSS—IT Modernization (ITM) (P)	X

¹ (P) indicates Program.

² (S) indicates Services.

³ Per I&A, OTIS Program has been canceled.

Question. The request includes \$24.2 million and 150 positions to strengthen the Department's acquisition workforce. Based on the Department's assessment of its acquisition workforce, does the request completely fill the gap in acquisition workforce needs? What is the long-term plan to address known gaps?

Answer. The 150 positions are based on a survey conducted in fiscal year 2010 of the major acquisition programs and acquisition oversight offices to identify gaps in the acquisition workforce and represent the number of positions required to fill gaps to ensure successful program execution, including risk mitigation.

DHS continues our concerted recruitment efforts with the use of direct hire authority and centralized vacancy announcements. As of December 31, 2010, these efforts have resulted in a 136 percent increase in our contracting specialists. We are also graduating the first 30 Acquisition Professional Career Program participants in fiscal year 2011 who will be trained, certified contracting specialists and placed within the Department's nine contracting activities throughout fiscal year 2011. Additionally, we have expanded the Acquisition Professional Career Program to include additional fields in program management, business cost estimating, systems engineering, life-cycle logistics, and information technology. DHS has also established new certification programs for the test and evaluation, logistics, business cost estimating, and acquisition financial management career fields, and will have new programs in place in fiscal year 2012 for systems engineers and information technology specialists.

Question. What is the status of the Department's plans to develop a formal Technology Readiness Level (TRL) process? The purpose of the process is to require TRL assessments of chemical, biological, radiological, nuclear detection, and other technologies prior to appropriate acquisition decision points. Has a management directive on this initiative been finalized? If so, provide a copy to the subcommittee.

Answer. The Science and Technology Directorate (S&T) Office of Acquisition Support and Operations Analysis is dedicated to assisting the DHS components with their acquisition programs, including test and evaluation master plans, systems integration and technology maturity assessments. This office is charged with engaging the components and executing S&T's portions of Acquisition Directive 102-01 and facilitating the deployment of technology. There is no current plan to create a separate TRL Management Directive.

—DHS TSD/DOT&E has been closely involved with SBInet throughout the acquisition process:

- Assisted with developing an integrated T&E strategy for SBInet as codified in the DHS Director, Operational Test and Evaluation's (DOT&E) approved test and evaluation master plan.
- Assisted with selection of, and ultimately approved the Army Test and Evaluation Command (ATEC) as the Operational Test Agent (OTA), an agency with demonstrated capabilities in the test and evaluation of command and control and surveillance systems.
- Observed SBInet user assessment testing at Playas, New Mexico. Reviewed developmental testing documentation related to test and evaluation at the

system and subsystem levels, to help ensure both the credibility of T&E results and the confidence in the understanding of system performance and overall system maturity.

- Participated in SBInet monthly program reviews.
- Member of the SBInet AoA Executive Leadership Team and Working Group.
- Participated in SBInet's operational test readiness review and Acquisition Review Board providing risk information to program executives and decision-makers.
- Approved ATECs operational test plan for SBInet Tucson One sector.
- Observed and monitored SBInet TUS1 Operational Testing (OT) and OT dry run (mid-October 2010 through mid-November 2010).
- Participated in ATEC's OT emerging results briefing on March 2, 2011. The final OT evaluation report is due early April 2011.
- Drafting DOT&E's Letter of Assessment (LOA) that assesses the adequacy of the Army's independent operational test and evaluation results. This LOA will be submitted to the Under Secretary for Management and used to support future decisions on border technologies.
- Currently working with Customs and Border Patrol on the Land Border Integrated Fixed Tower program to ensure adequate test and evaluation is planned, executed and reported as required by DHS directive.

WORKFORCE BALANCING

Question. What is the total number of contractor full time equivalents (FTE) providing services in support of DHS programs? Across departmental components, the request proposes to move resources from contract service providers to in-house staff. Provide a departmentwide chart for this effort by component for fiscal year 2011 and fiscal year 2012, including the shift in personnel from contractor to Federal FTE and associated cost savings. Since the Balanced Workforce Strategy began, how many contractor conversions has the Department realized? How will you measure the success of the Balanced Workforce Strategy?

Answer. After the Balanced Workforce Strategy (BWS) Departmental Working Group was formed, it reviewed information provided by the firm (LMI) that developed the algorithm and identified a math error that caused the number of contractors to be significantly overstated. The Department worked with the firm to reexamine the algorithm and assumptions. The firm informed the Department that the initial 210,000 contractor work-year equivalent estimate was overstated by 100,000 or more.

The BWS Tool, an automated survey that leads a component official through the analysis process of the Department's contracts and mission needs, is a key element of our strategy to reduce expenditures on professional services contracts in order to more effectively and efficiently achieve our mission.

Some of the results of our efforts thus far include reducing spending on professional services contracts by 11 percent, or \$420 million, from fiscal year 2009 to fiscal year 2010. The Department's fiscal year 2012 budget request includes an additional \$106 million in cuts to professional services contracts across the Department, demonstrating our commitment to better managing contracts and ensuring the appropriate mix of personnel.

Ultimately, the BWS will be considered successful if it:

- Ensures compliance with current statutes, regulations, and Government and DHS policies by documenting components' reviews of current contracts; and
- Objectively assesses the proper sourcing decisions for performing work that advances the mission of the Department of Homeland Security.

SMALL BOAT STRATEGY

Question. The Department released its small vessel security strategy on April 28, 2008. Nearly 3 years later, an implementation plan to carry out the strategy has not been released. In response to a question for the record from the Secretary's 2010 budget hearing, the subcommittee was informed that the Department of Homeland Security Small Vessel Security Implementation Plan was to be released in 2010. When will the implementation plan be provided to the Congress?

Answer. The Small Vessel Security Strategy Implementation Plan was released on March 11, 2011. The public report is available on the DHS Web site at: http://www.dhs.gov/files/programs/gc_1299623119339.shtm.

AIR DOMAIN AWARENESS—C2 GAP FILLER

Question. The request includes \$11 million for an air domain awareness initiative called C2 Gap Filler. Does this program replicate existing DHS capabilities? If not,

what additional benefits to DHS would this program provide if successful? The total DHS contribution to this multi-agency effort is \$16 million, but only \$11 million has been identified. The Operations Coordination budget request indicates that the \$11 million is a “one-time” cost. How will the Department pay for the remaining \$5 million? If approved, what are the additional costs in fiscal years 2013–2016?

Answer. [Follows:]

State and Local Efforts

The Department of Homeland Security’s (DHS) National Cyber Security Division (NCSD) collaborates with State, local, tribal, and territorial governments to share and implement sound cybersecurity policies, practices, and strategies to improve preparedness against cyber threats and attacks.

Due to the increasingly important role of State, local, tribal, and territorial governments in cybersecurity, NCSD has resources committed solely to interacting with officials at these levels. The mission of NCSD’s State, Local, Tribal, and Territorial (SLTT) Engagement program is to build partnerships with non-Federal public stakeholders, including each State’s Homeland Security Advisor, Chief Information Officer (CIO) and Chief Information Security Officer (CISO). The following provides an overview of NCSD interactions with States.

United States Computer Emergency Readiness Team

The United States Computer Emergency Readiness Team (US-CERT) maintains a formal relationship and works closely with mission partners, including State and local governments, on a daily basis to resolve threats, vulnerabilities, and incidents. US-CERT provides a variety of daily, weekly, monthly, and quarterly communication exchanges to maintain situational awareness and share critical information with collective cybersecurity partners. Federal and SLTT incident response personnel have access to the Government Forum of Incident Response and Security Teams (GFIRST) portal for information sharing and discussion.

US-CERT also sponsors the GFIRST National Conference, a forum that promotes cooperation among Federal agencies, State, local, tribal, and territorial governments, the private sector, and international partners across the cybersecurity spectrum, from preparedness and prevention to incident response. The conference supports the dissemination and promulgation of proactive and preventive security practices. US-CERT funding is executed toward planning, preparation, communication, and coordination of this conference and other conference expos. Specifically, \$1.55 million is directed to support requirements such as administration, logistics, and security. Additional funding (approximately \$3 million) provides support to the interactive demonstration system at the GFIRST National Conference.

US-CERT also provides support (\$1 million annually) to the Department of Commerce’s National Institute of Standards and Technology, which provides system integration and product development support for enhancement of the National Vulnerability Database and search engine. This database enables US-CERT partners, including State, local, tribal, and territorial governments, to secure government systems.

Multi-State Information Sharing and Analysis Center

Created in 2003, the Multi-State Information Sharing and Analysis Center (MS-ISAC) is an invaluable tool when dealing with SLTT governments. The MS-ISAC supports NCSD’s efforts to secure cyberspace by disseminating early warnings of cyber threats to SLTT governments. In addition, the MS-ISAC shares security incident information, identifies trends, and conducts other analysis for security planning. NCSD provides programmatic support (\$3.55 million for the 12-month period from August 1, 2010, to July 31, 2011) to the MS-ISAC. The fiscal year 2010 DHS appropriations act provided an additional \$3 million for DHS to fund and work with the MS-ISAC to provide managed security services (e.g., intrusion detection systems, intrusion prevention systems firewalls) for 18 State and local governments. The MS-ISAC has selected State, county, and local governments for participation. The MS-ISAC, consistent with the objectives of NCSD, provides a common mechanism for raising the level of SLTT government cybersecurity readiness and response. It is a central resource for gathering information regarding cyber threats to critical infrastructure facilities. Other MS-ISAC programs/activities include:

—*Operation of a 24/7 Cyber Security and Analysis Center.*—The MS-ISAC runs a 24-hour watch and warning Security Operations Center (SOC) that provides real-time network monitoring, dissemination of early cyber threat warnings, and vulnerability identification and mitigation, along with education and outreach aimed at reducing risk to the Nation’s SLTT government cyber domain. The SOC shares and coordinates real-time risk information to support national cybersecurity situational awareness with DHS (NCSD and US-CERT).

The SOC performs 24/7 monitoring of the Internet and other sources, including incident reports received from members and others regarding cybersecurity threats and vulnerabilities. The SOC staff evaluates and correlates information and distributes advisories and bulletins as appropriate, including mitigation strategies and steps that can be taken to protect critical infrastructure.

—*Managed and Monitored Security Services.*—The MS-ISAC contracts with the States of Alaska, Montana, and New York, along with the Los Angeles World Airports, to provide cybersecurity monitoring and managed services. This collective view across multiple entities helps enhance situational awareness regarding cyber threats.

During 2010, the MS-ISAC reviewed more than 78 billion logs through the 24/7 operations center. Approximately 138 MS-ISAC advisories were issued.

Additionally, through funding in the fiscal year 2010 DHS appropriations act, the MS-ISAC is expanding its monitoring services with an additional 10 State governments, 7 local governments, and 1 territorial government. This expanded infrastructure will provide a representative sample of system and network activity for enhancing situational awareness of SLTT government networks across the country. It will also improve cyber incident identification and response while providing more resources for developing and implementing appropriate mitigation strategies tailored specifically to SLTT government cyber resources.

—*Participation in Cyber Security Exercises—Cyber Storm I, II, and III.*—The MS-ISAC has participated in each of the three Cyber Storm exercises, most recently Cyber Storm III in September 2010. The MS-ISAC was a full player during the Cyber Storm III exercise; its SOC was active, and it coordinated with 11 States that participated in the exercise. The MS-ISAC hosted 19 visitors from five States, the Federal Bureau of Investigation, New York State law enforcement, Homeland Security and military personnel, and observers from the University of Texas at San Antonio.

National Cyber Incident Response Plan

The President's Cybersecurity Policy Review called for "a comprehensive framework to facilitate coordinated responses by Government, the private sector, and allies to a significant cyber incident." DHS coordinated the interagency, State and local government, and private-sector working group that developed the National Cyber Incident Response Plan (NCIRP). The plan provides a framework for effective incident response capabilities and coordination among Federal agencies, State and local governments, the private sector, and international partners during significant cyber incidents. It is designed to be flexible and adaptable to allow synchronization of response activities across jurisdictional lines.

The NCIRP is undergoing final DHS review to incorporate lessons learned during the Cyber Storm III exercise. Upon conclusion of this review, DHS will send the NCIRP out to State, local, and private-sector partners (including the National Governors Association and the MS-ISAC) for review. DHS will work with State and local partners (and partners in the private sector) to align their incident response plans and procedures with the NCIRP. The MS-ISAC and National Governors Association will be key partners in this effort.

DHS has designated the MS-ISAC as the ISAC for SLTT governments and has identified the MS-ISAC as a key stakeholder in the development and implementation of the NCIRP.

NCSD Cyber Security Evaluation Program

Under the 2009 Appropriations Act, NCSD's Cyber Security Evaluation Program (CSEP) was tasked with completing a Nationwide Cyber Security Review (NCSR). The NCSR is a voluntary self-assessment of State and major urban area government Information Technology (IT) services and is designed to measure cybersecurity preparedness and resilience. Through the NCSR, CSEP examines relationships, interactions, and processes governing IT management and the ability to manage operational risk effectively. CSEP also conducts voluntary cybersecurity assessments to evaluate and enhance the implementation of key cybersecurity capacities and capabilities of Critical Infrastructure and Key Resources (CIKR) Sector members. This assessment is the Cyber Resilience Review, which is designed for each of the 18 CIKR Sectors and for use within SLTT governments. Since fiscal year 2009, CSEP has completed 45 cyber resilience reviews with SLTT partners.

NCSD Cyber Exercise Program

NCSD's Cyber Exercise Program (CEP) works with Federal, State, local, international, and private sector partners to conduct regional and sector-specific exercises designed to develop and improve the capabilities of DHS and its infrastructure partners. Such exercises aid participants in preparing for, preventing, mitigating,

responding to, and recovering from cyber incidents. NCSD plans, coordinates, and conducts cyber exercises to develop, evaluate, improve, and refine the capabilities of State and local partners. CEP assists State and local partners by facilitating the design of tabletop and functional exercises at the State and local levels.

DHS hosted Cyber Storm III from September 26, 2010 through October 1, 2010. The Cyber Storm exercise series is a key element of ongoing efforts to assess cyber preparedness; examine incident response processes, procedures, and information sharing mechanisms; and identify areas for improvement absent the consequences of an actual incident. Cyber Storm III included participation from 11 States.

In 2009 and 2010, NCSD, the MS-ISAC, and the Microsoft Corporation jointly sponsored the Defend the Flag Exercises to provide State government network security professionals greater technical security skills and practical experience with implementing the principles of defense-in-depth while securing Windows-based operating systems. Thirteen States participated from 2009–2010.

Grants

DHS provides grants for cybersecurity through the Federal Emergency Management Agency (FEMA), such as the Homeland Security Grant Program (HSGP), which provides States the opportunity to work with DHS to acquire cybersecurity capabilities. During the last 2 years, NCSD has worked with FEMA to modify the language in the HSGP to better clarify how funds can be used to improve cybersecurity.

National Initiative for Cybersecurity Education

DHS is engaged in the National Initiative for Cybersecurity Education (NICE), leading Track 1 (Cybersecurity Awareness), leading Track 3 (Cybersecurity Workforce Structure), and coleading Track 4 (Cybersecurity Workforce Training and Professional Development). Through NICE, DHS is reaching out across the cybersecurity community—including academia, the private sector, and Federal, State, local, tribal, and territorial partners—to integrate current efforts into a foundation of information that creates mutual understanding and partnerships across all aspects of national cybersecurity.

In fiscal year 2010, DHS facilitated the efforts of six State government CIOs to develop a State government workforce development model, based on the existing DHS-issued Essential Body of Knowledge. This State government model was presented to the MS-ISAC, which included the model in its membership-based portal and on its public Web site.

Other NCSD SLTT Programs/Activities

—*National Cyber Security Awareness Month.*—To recognize the importance of cybersecurity awareness, October is designated as National Cyber Security Awareness Month. NCSD, with the help of the MS-ISAC, works with funded partners and other parties to sponsor events and activities throughout the country and disseminate Awareness Month key messages and event information to State and local partners. Due to the efforts of NCSD and MS-ISAC, in 2009 and 2010, all of the Nation's Governors signed letters officially proclaiming October as National Cyber Security Awareness Month.

—*Stop. Think. Connect. Campaign.*—DHS bears primary responsibility for raising public awareness about threats to the Nation's cyber systems and networks. To that end, in October 2010, DHS launched the National Cybersecurity Awareness Campaign, Stop. Think. Connect. It is a national public-education effort to engage and empower Americans to take charge of their online safety and security. By providing Americans with easy-to-understand online safety tips and resources, the campaign is helping them establish smart habits that will lead to increased protection online. Stop. Think. Connect. fulfills a key element of President Obama's 2009 Cyberspace Policy Review, which tasked DHS to develop a public-awareness campaign to inform Americans about ways to use technology safely.

—*Security Clearances for State Information Security Officers.*—NCSD, in partnership with colleagues from DHS Office of Security, initiated a plan to clear, starting at the secret level, each State CIO and CISO, and the MS-ISAC executive committee. NCSD is confident this is an important step in sharing valuable sensitive information with State partners.

—*Cyber Partner Local Access Plan.*—NCSD, in cooperation with the Office of Intelligence and Analysis, developed the Cybersecurity Partner Local Access Plan (CPLAP) to share classified cybersecurity threat information with cleared State cybersecurity officials and private-sector partners at State and major urban area fusion centers nationwide. The CPLAP enables more effective and efficient classified cybersecurity information sharing among Federal, SLTT, and private-

sector partners, and supports an information-sharing model that eliminates partners' air travel to and from the Washington, DC, area to receive classified cybersecurity briefings. The CPLAP will be piloted at five fusion centers by mid-2011, with plans to expand the program to a broader audience and additional fusion centers on a regional basis by the end of 2011.

—*Cyber Summits.*—In an effort to educate SLTT leaders and the public, NCSD coordinates and plans Cyber Summits. These summits, which are held regularly throughout the year and hosted across the country, focus on opportunities and vulnerabilities to promote discussion on how public and private-sector officials can best leverage technology to reduce risk. Frequent attendance and contribution by nongovernmental cyber associations, such as the MS-ISAC and National Association of State Chief Information Officers, significantly contributes to the information sharing, capacity building, and coordination efforts necessary to develop robust and effective cybersecurity capabilities on all levels. DHS identified cybersecurity as a top departmental priority, and Federal, State, and local government officials share a responsibility to promote a healthy cyber ecosystem and to encourage individuals to protect themselves and their families at home, work, and school.

—*Virginia Operational Integration Cybersecurity Center of Excellence.*—NCSD is helping the Virginia Operational Integration Cyber Center of Excellence (VOICCE) create a Municipal Cyber Lab that will be used to support and train SLTT government officials to better understand cybersecurity issues. VOICCE focuses on incorporating cyber attacks into the mainstream of emergency operations at the local level and creating a virtual municipality of randomly generated Internet protocol addresses. The concept will allow for development of vital cybersecurity capabilities, processes, and procedures. The VOICCE node or laboratory will allow local governments and first responders to plug into State and Federal entities and participate in simulated cyber attacks. The lab will be both physical and virtual in structure, allowing many types of simulation and providing an effective environment to share ideas among stakeholders across the Nation. Participants will brainstorm, identify, and respond to diverse cyber attack scenarios.

This activity was required by the fiscal year 2010 Department of Homeland Security Appropriations Act.

NCSD will continue many of the programs listed above. In addition, in fiscal year 2012, NCSD will commit funding to expand the MS-ISAC's managed and monitor security services.

Curricula

The Software Assurance (SwA) curriculum project, which produced the Masters of Software Assurance (MSwA) curriculum and associated undergraduate course outlines, is a recent NCSD effort to cosponsor public-private collaboration for government, industry, and academia through its SwA forum. To facilitate implementation, the MSwA project team is offering assistance, free of charge, to educational institutions looking to launch an MSwA degree program.

Through the Software Assurance (SwA) forum, the SwA program has encouraged Federal, State, and local involvement in public-private collaboration efforts associated with the advancement of SwA resources. As part of that collaboration, the SwA curriculum project released the Masters of Software Assurance (MSwA) reference curriculum and nine-course syllabi for public use. The MSwA curriculum is recognized by the Institute of Electrical and Electronics Engineers (IEEE) Computer Society and the Association of Computing Machinery (ACM) as the first curriculum of its kind to focus on assuring the functionality, dependability, and security of software and systems. The materials are available at <http://www.cert.org/mswa/>.

More information on the SwA Curriculum Project and the MSwA is available at <https://buildsecurityin.us-cert.gov/bsi/1165-BSI.html>.

Virtual Education

The SwA forum, sponsored by NCSD's SwA program, posts Web casts of SwA tutorials and pocket guides that are publicly available for free online use, including links via virtual training environments.

One aspect under NICE track 4 is functional area 4, which concerns specialized cybersecurity operations. The scope of this effort includes those Federal civilian employees, members of the uniformed services, and contractor personnel employed by departments and agencies who are engaged in highly specialized and largely classified cybersecurity operations. Work associated with this functional area is classified, but a classified briefing to discuss the work associated with this topic can be arranged upon request.

HOMELAND SECURITY INFORMATION NETWORK

Question. Please describe the Department's efforts to consolidate DHS information portals into the Homeland Security Information Network. How many portals will migrate to HSIN in fiscal year 2011 and how many are anticipated to migrate in fiscal year 2012? What are the cost savings associated with the migrations in fiscal year 2011 and fiscal year 2012 as well as the long-term cost savings for other portals?

Answer. The Department plans to migrate three portals in fiscal year 2011, and seven portals in fiscal year 2012. Details on the portals to be consolidated, as well as 1-year savings and the 5-year savings by portal are provided below. We continue to evaluate other portals for migration to HSIN.

HSIN PORTAL CONSOLIDATION AND PROJECTED COST-SAVINGS

Portal name	Year 1 savings	Total 5-year savings	Target year
FISCAL YEAR 2011			
Fire Services Portal	\$200,000	\$1,000,000	Fiscal year 2011 (completed)
TSA—Exercise Information System (EXIS)	132,760	1,075,092	Fiscal year 2011
NPPD—Federal Protective Service (FPS) Secure Portal	(350,284)	2,310,491	Fiscal year 2011
FISCAL YEAR 2012			
I&A—Homeland Security—State and Local Intel Community (HS-SLIC)	673,368	6,428,728	Fiscal year 2012
NPPD—National Cybersecurity Protection System (NCPS)	1,410,103	10,941,546	Fiscal year 2012
FLETC—FLETC Partners and FLETC Registration ¹	(1,563,498)	(659,896)	Fiscal year 2012
DNDO—Joint Analysis Center Collaborative Information System (JACCIS)—Partial Consolidation	500,000	1,300,000	Fiscal year 2012
FEMA—Homeland Security Exercise Evaluation Program—Corrective Action Planning System (HSEEP—CAPS)	2,148,402	5,713,724	Fiscal year 2012
NPPD—Technical Resource for Incident Prevention (TRIPwire)	(1,575,548)	2,125,952	Fiscal year 2012
USCG—HomePort Portal	(680,232)	12,412,802	Fiscal year 2012
Totals	895,072	42,648,440	

¹ Pending verification of FLETC portals budget figures.

FINANCIAL SYSTEMS CONSOLIDATION

Question. Please provide an update on the Department's efforts to implement the recommendations made in the July 2010 Inspector General's report on the transformation and systems consolidation effort.

Answer. Through extensive efforts with the CFO, CPO, CIO, CAO and DHS components over the past year, we have made significant progress in DHS's integrated financial acquisition strategy.

The Department has clearly defined and documented its strategy, plan, and concept of operations in the TASC program management documentation. To help ensure the success of the program, the Department formulated a number of cross-functional oversight and management mechanisms for TASC, including the TASC Executive Steering Committee (ESC) which is chaired by the USM, that serves as the governing board regarding strategy, policy, funding, and risks for the TASC program.

The TASC procurement strategy was a single-award IDIQ contract allowing multiple contract types for task orders (firm fixed price, time and materials, cost plus award fee, and cost plus fixed fee).

On November 19, 2010, DHS issued a contract for the TASC program. However, on March 9, 2011, DHS received the decision from the GAO that while two protests to the TASC contract had been dismissed, one had been upheld. In light of the GAO ruling a stop work order was issued for the TASC IDIQ contract and for the first task order on that contract. We are currently assessing GAO's findings and recommendations to determine the appropriate way forward.

ICEBREAKING ACQUISITIONS ANALYSIS

Question. The funding request for the icebreaking acquisition analysis will not be considered until the Polar High Latitude Study is submitted to the subcommittee.

Please provide a summary of the “numerous existing and ongoing studies” referenced in the budget request. How will this study be different than those studies? What is the \$5 million request based on? How will the funding be used? Why has the High Latitude Study, which was funded in the fiscal year 2009 budget request, been delayed? When will it be submitted to the subcommittee?

Answer. The most recent of the studies referenced in the budget justification was completed in 2007 at the request of the Coast Guard by the National Academy of Sciences sponsored by the National Research Council. This study’s objective was to assess Coast Guard’s polar icebreaker roles and future needs. Additionally, the Department of Homeland Security’s Office of Inspector General recently completed an analysis to assess Coast Guard’s polar icebreaking missions.

This polar icebreaking analysis will differ from those studies by taking a broader look at polar icebreaking requirements across all Federal agencies, and by taking a deeper look at operational alternatives to determine the best method to deliver the required capability. The closest model for this effort is the Polar Icebreaker Requirements Report prepared for the President in 1990. Fiscal year 2012 funding will support an interagency working group to define Terms of Reference and the approach to be used for the preacquisition analysis of 21st century icebreaking capabilities. The working group will be under the direction of the Under Secretary for Management.

The \$5 million request for the Icebreaker Acquisition Analysis is based on historical costs of analyses with similar size and scope.

The results of the High Latitude Study have been compiled by Coast Guard and their summary report is currently in the final stages of review and will be provided to the subcommittee in the near future.

Question. Included in the amount appropriated in fiscal year 2010 for Polar Icebreaker Sustainment was funding for the Coast Guard to begin a business case analysis for either a new heavy polar icebreaker class or a major service life extension project for existing polar icebreakers. What is the status of this effort?

Answer. The Coast Guard-specific business case analysis directed in the fiscal year 2010 appropriation is in final review. The President’s fiscal year 2012 budget request includes funding for the completion of a Government-wide analysis for future icebreaking requirements in the polar regions. Acquisition of 21st century icebreaking capabilities will be based on these final requirements.

OFFICER INTEGRITY

Question. Since fiscal year 2006, with the support of this subcommittee, U.S. Customs and Border Protection (CBP) has hired 16,000 new employees—a 37 percent increase. U.S. Immigration and Customs Enforcement (ICE) has hired more than 8,200 new personnel—a 31 percent increase. This subcommittee has been concerned that due to the rapid hiring at CBP and ICE, there is a potential for increased opportunities for officer corruption. Toward that end, for the past 3 years, this subcommittee has provided additional resources for integrity training, investigations of misconduct allegations, and background investigations. I am pleased to see that your budget requests an additional \$26 million for CBP to address these efforts and meet the legislative mandate of the Anti-Border Corruption Act of 2010.

This is the right thing to do and I support this funding. However, I understand that CBP, ICE, and the Inspector General are experiencing difficulties working together on workforce integrity because of an apparent lack of clear lines of authority regarding which departmental entity is to conduct differing types of investigations and when. There have been reports that a Border Patrol agent was charged with harboring illegal aliens but because the DHS Inspector General chose not to participate in a specific Border Corruption Task Force, the investigation into the alleged activity was impeded.

The American taxpayer’s trust in the integrity of Federal law enforcement officers is too important to be subject to stovepipes and petty bureaucratic behavior in Washington. In your response to my question during the hearing, you indicated that this was a priority for your Department and that you and the Deputy Secretary would commit to work with me on establishing clear lines of authority for integrity investigations.

What specific steps have been taken in this regard to date and what further actions can your Department take to improve this process? Please provide a schedule for this review and a date by which you or the Deputy Secretary will report back to the subcommittee on the recommendations to improve the process. What additional funds beyond the \$26 million requested in the fiscal year 2012 request are required for full implementation of the Anti-Border Corruption Act?

Answer. We are fully committed to fighting corruption and maintaining the integrity of our workforce across the Department. The President's fiscal year 2012 budget request provides sufficient funding for workforce integrity in support of the Anti-Border Corruption Act (Public Law 111-376). The request includes a \$26 million enhancement for CBP to enhance its polygraph program and ensure timely background and periodic reinvestigations as mandated by the Anti-Border Corruption Act of 2010 while maintaining all other aspects of CBP's integrity programs, including oversight of CBP operations, personnel, and facilities. Resources will also be used to improve the Office of Internal Affairs' ability to detect and deter insider and cyber threats, including the growing threats posed by Foreign Intelligence Services, terrorists, and foreign criminal organizations. Additionally, the base budget requests for CBP and ICE include \$142 million and \$94 million, respectively, to support anticorruption activities.

DHS and our components have taken several actions to ensure that all parts of the Department are working together effectively to fight corruption.

First, in 2004, CBP and ICE created the Joint Intake Center (JIC), which was designed to serve as the central clearinghouse for receiving, documenting, and processing all allegations of misconduct involving ICE and CBP employees and to ensure that the Office of the Inspector General (OIG) receives appropriate and timely notification through the Joint Integrity Case Management System (JICMS).

Second, I have directed CBP and ICE to adhere to the DHS Management directive, which requires CBP and ICE to promptly advise the OIG regarding allegations of employee misconduct. CBP leadership has taken prompt action to ensure strong cooperation between CBP's Office of Internal Affairs (CBP IA) and OIG. In October 2009 and July 2010, CBP IA issued guidance to all CBP IA special agents-in-charge requiring that detailed information regarding any allegation of wrongdoing on the part of a CBP employee be entered into JICMS on the same day or the day after receiving the information. The guidance extends specifically to CBP IA agents serving on Border Corruption Task Forces (BCTFs).

Third, this past January, CBP and ICE entered into a Memorandum of Understanding (MOU) establishing a program whereby CBP would augment ICE investigations of criminal misconduct by CBP employees through the detail of CBP IA agents to ICE's Office of Professional Responsibility. Since the MOU became effective on January 1, 2011, CBP has detailed 24 special agents to ICE OPR. Pursuant to the MOU, CBP IA has begun working collaboratively with ICE OPR on 160 potential criminal cases targeting CBP personnel.

The Department will continue to work closely with its components and OIG to ensure allegations of fraud, waste, and abuse, as well as allegations of corruption within the DHS workforce, are addressed in an effective and timely manner. We will continually review our processes for ensuring officer integrity, and make any adjustments to those processes as necessary.

REAL ID ACT COMPLIANCE

Question. This subcommittee has committed significant resources to make driver's licenses and identification cards more secure. This security measure was recommended by the 9/11 Commission and is required through the REAL ID Act. Of the \$190 million appropriated to FEMA for REAL ID-related grants to date, approximately \$161.2 million has been obligated to individual States for security improvements to individual State credentials and licensing processes and \$28.8 million to information sharing and verification capability improvements. Of the \$60 million appropriated to USCIS, approximately \$6.3 million has been obligated by USCIS to immigration status verification projects and \$28.5 million has been obligated to FEMA to supplement existing FEMA grants for information sharing and verification capability improvements. On March 7, 2011, the date for final compliance with the REAL ID Act was changed from May 11, 2011 to January 15, 2013 through a Federal Register notice. The change was made citing the difficulty States are still having meeting all of the statutory requirements. The notice also recognizes significant progress has been made by States in some areas.

Please provide a copy of the notice for the record.

How many States are currently in compliance with the act, how many are expected to be in compliance this fiscal year, and how many are estimated to be in compliance in fiscal year 2012?

Please outline why the Nation is safer because of the investments and progress made to date and detail how the fiscal year 2012 budget request continues the progress of this effort. Will the Department resubmit PASS ID?

Answer. [The final rule is available at <http://www.gpo.gov/fdsys/pkg/FR-2011-03-07/pdf/2011-5002.pdf> (Federal Register/Monday, March 7, 2011/Vol. 76/No. 44/pgs 12269–12271/Rules and Regulations).]

To address concerns raised by the States over various aspects of REAL ID, DHS supported PASS ID legislation introduced in the last Congress. PASS ID would have made a number of changes to the REAL ID Act to facilitate State compliance. Since this bill was not approved by the Congress we have made considerable progress in implementing REAL ID.

To date, five States have submitted for DHS review, full-compliance certification packages. Additionally, a number of States are making progress in meeting the requirements of the REAL ID Act. A majority of States have self-certified that they either already or plan to: verify lawful status using the Systematic Alien Verification for Entitlements (SAVE) system; conduct background checks and fraudulent document training for employees; incorporate safeguards to improve the physical security of driver's license production facilities; and implement technology linking DMV employees to the credentials they issue. Moreover, by the end of 2011, nearly all of the reporting States will have implemented additional security enhancements related to DMV employees, physical security, technology, and card security. By implementing these security enhancements, States can more effectively mitigate fraud associated with State-issued credentials, and make it more difficult for individuals to obtain identity documents they are not entitled to.

REAL ID STATUS OF STATES AS OF MARCH 29, 2011¹

States that have submitted full compliance certification packages to DHS (5).	Maryland, Tennessee, Connecticut, South Dakota, Delaware.
States issuing materially compliant documents with gold star (4) (Self-certified).	Alabama, Florida, Indiana, Utah.
States that are materially compliant but not issuing compliant gold star documents (7) (Self-certified).	Arkansas, District of Columbia, Iowa, Kansas, Kentucky, Mississippi, New Jersey.
States committed to meet material compliance but need additional time (12).	Colorado, Hawaii, Illinois, Nebraska, Ohio, Puerto Rico, Rhode Island, Texas, Virginia, West Virginia, Wisconsin, Wyoming.
States with comparable EDL programs (4)	New York (issues EDL), Michigan (issues EDL), Vermont (issues EDL), <i>Washington (issues EDL)</i> .
States committed to meet 15 of 18 benchmarks (12)	<i>Arizona, California, Georgia, Minnesota, Missouri, Nevada, New Hampshire, North Carolina, North Dakota, Pennsylvania, South Carolina, Virgin Islands.</i>
States that have indicated they will not meet four or more benchmarks within the next 12 months (12).	<i>Alaska, American Samoa, Guam, Idaho, Louisiana, Maine, Massachusetts, Montana, New Mexico, Oklahoma, Oregon, Northern Marianas.</i>

¹ This information was compiled from documentation submitted by the States in response to DHS requirement to submit Material Compliance benchmark data or Full Compliance Certification information. All of the information is self-reported by the States so all conclusions based on this information may not accurately reflect a State's actual progress in complying with the requirements of the REAL ID regulation.

Note: *Italic text* denotes States with legislation preventing REAL ID compliance.

States may use funds provided through the State Homeland Security Grants Program to continue to improve the security of their driver's license program.

COORDINATION OF FEDERAL CHEMICAL SECURITY EFFORTS

Question. The Senate Report (111–31) accompanying the fiscal year 2010 Department of Homeland Security Appropriations Act (Public Law 111–83) directed the Department to report quarterly on its efforts to coordinate chemical security across departments. The fourth quarter report received on March 4, 2011 outlines several memorandums of agreements, regulatory reviews, and regulatory amendments that are under development. Please provide a specific timeline for each of these efforts and identify any obstacles to meeting the timelines expeditiously. In particular, please update the subcommittee on efforts to establish standardized risk assessments for facilities under the Maritime Transportation Security Act and the Chemical Facilities Anti-Terrorism Standards.

Answer. [Follows:]

Infrastructure Protection / United States Coast Guard Coordination

The National Protection and Programs Directorate's (NPPD's) Office of Infrastructure Protection (IP) and the United States Coast Guard (USCG) continue to work toward harmonization of the Chemical Facility Anti-Terrorism Standards (CFATS)

and Maritime Transportation Security Act (MTSA) regulatory programs under the auspices of the chartered CFATS–MTSA Harmonization Working Group. In November 2010, senior leadership from NPPD and USCG signed the charter. As stated in the activities detailed in the Fourth Quarter Report to Congress, the CFATS–MTSA Working Group continued “the development of a full regulatory review of the security regimes established under MTSA and CFATS.”

In November 2010, the Working Group presented a comprehensive regulatory review to NPPD Under Secretary Rand Beers and Rear Admiral (RADM) Brian Salerno, the USCG Deputy Commandant for Operations. This review was designed to inform leadership regarding options for seeking consistency of security across all high-risk chemical facilities. The findings of this review have been approved by NPPD/IP and USCG leadership; NPPD/IP’s Infrastructure Security Compliance Division (ISCD) and USCG are currently working to further a number of initiatives both independently and through the Working Group and designated subgroups. Also noted in the Fourth Quarter Report to Congress, NPPD and USCG are working toward the “Refinement of a [Memorandum of Agreement (MOA)] to enable data sharing and sharing of risk methodologies between ISCD’s Chemical Security Assessment Tool and USCG’s Maritime Security Risk Analysis Model” Consistent with the findings and recommendations of the Working Group, NPPD and USCG are establishing a Risk and Information Sharing Sub-Group designed to complete development of the referenced MOA, which will relate to the exchange of specific risk information and an assessment of the approaches to risk management currently employed by ISCD and USCG for their respective programs. Execution of the MOA is expected by summer 2011.

In order to help DHS develop a more comprehensive picture of security issues at the Nation’s chemical facilities, and to help DHS evaluate whether any regulatory gaps exist that may pose an unacceptable security risk, the Department has begun the process, with close cooperation between NPPD and USCG, for determining whether and how to require MTSA-covered facilities that possess CFATS chemicals of interest to complete and submit CFATS Top-Screens.

DHS/Federal Bureau of Investigation Coordination.—With regard to the Department’s efforts to coordinate with the Federal Bureau of Investigation (FBI), NPPD is developing an operational-level MOA with the FBI specific to chemical security and related national security issues. As noted in the Fourth Quarterly Report to Congress, “This MOA will establish proactive guidelines that build upon our current working relationships and allow for additional interagency activities (such as information sharing on high-risk chemical facilities and field component interaction) and will resolve any potential jurisdictional issues proactively.” As the MOA is developed, NPPD/IP and the FBI are also leveraging a formal agreement, entered into between the Department’s Office of Intelligence and Analysis and the FBI in September 2010, regarding the development of joint intelligence products (such as intelligence bulletins). NPPD/IP and the FBI are currently leveraging this agreement in relation to products jointly developed for chemical security-related issues.

DHS/Nuclear Regulatory Commission Coordination

As stated in the Fourth Quarterly Report to Congress, “At the staff level, DHS and the [Nuclear Regulatory Commission (NRC)] finalized and submitted to DHS and NRC leadership for review and execution a jointly developed draft Memorandum of Understanding (MOU) designed to help define the types of facilities that are wholly or partially exempt from CFATS due to NRC-regulatory authority, as well as processes for identifying those facilities.” NPPD Under Secretary Rand Beers formally endorsed the DHS–NRC MOU in August 2010, and the MOU is currently with NRC senior leadership for final review and execution.

OFFICE OF THE INSPECTOR GENERAL (OIG)

Question. In January 2011, a San Diego-area Border Patrol agent, Marcos Manzano was arrested for harboring illegal immigrants. One of the OIG’s missions is to investigate allegations of criminal, civil, and administrative misconduct involving DHS employees, and to work with the U.S. Attorneys, other law enforcement agencies, and investigate activities of DHS Internal Affairs offices to ensure violators are prosecuted, fined, and/or civil action is taken. In this particular case, the FBI Border Corruption Task Force (BCTF) had the lead on the investigation, but reports show that the DHS OIG was not involved due to the fact that the OIG has not signed on to the BCTF Memorandum of Understanding (MOU).

Why isn’t the DHS OIG part of the BCTF?

Answer. Despite the lack of any formal written agreement, DHS OIG has always tried to participate fully with the BCTF. Since its beginning in 2003, DHS OIG has worked cooperatively with the FBI and other law enforcement agencies on border

corruption matters involving DHS employees without any formal written agreement. In March 2010, DHS OIG assigned a Deputy Assistant Inspector General for Investigations to act as a liaison to the FBI's National BCTF in an effort to achieve full participation in all of the FBI BCTF's investigations. In addition, this Deputy Assistant Inspector General was tasked with negotiating an MOU that reflects the OIG's statutory responsibilities with respect to:

- Investigating allegations of criminal misconduct against DHS employees and
- Providing oversight of the internal affairs offices within DHS, while ensuring the representation of departmental interests in the course of these investigations.

In May 2010, the FBI in San Diego presented the OIG with an MOU that contained provisions that place significant restrictions on the OIG's independence, and were therefore unacceptable. We worked locally and at FBI headquarters to resolve differences and craft language to which all parties could agree. In November 2010, we proposed alternative language for the local BCTF MOU that both recognized the significance of border corruption offenses committed by DHS employees and respected the legislated authorities that define and govern roles and responsibilities of the member agencies that include the FBI, CBP Internal Affairs (IA), CBP Office of Field Operations (OPO), Border Patrol, and TSA Office of Investigations.

Our proposal was rejected by the FBI because the FBI failed to recognize that DHS has a system of tiered authority with respect to the investigation of allegations of criminal misconduct against DHS employees and that, within that system of tiered authority, OIG has primacy. Moreover, we were asked to remove the agent we had assigned to the San Diego task force because we had not signed the version of the MOU that was unilaterally drafted by the FBI. We honored the FBI's request and removed our agent on November 12, 2010. Since that time, several significant border corruption cases that DHS OIG has presented to the U.S. Attorney's Office in San Diego have been declined because the investigations were not conducted by the local BCTF.

The OIG has been prevented from participating in the FBI BCTF in San Diego because of the insistence that we sign an agreement we consider to be fundamentally flawed, and in conflict with our legislated mandate as the primary authority within DHS for investigating allegations that DHS employees have committed criminal misconduct. This authority is clearly specified in the Inspector General Act of 1978, as amended, and further articulated in the Secretary of Homeland Security's Management Directive (MD) 0810.1.

We have continued to negotiate with the USAO in San Diego to reach accord on an MOU that will preserve the OIG's independence and authority, but otherwise satisfies the general terms of the BCTF MOU. OIG continues to open and aggressively investigate all allegations relating to the corruption of DHS employees or the compromise of systems related to the security of our borders and transportation networks.

Question. Why hasn't the OIG signed the MOU? Is there something in the MOU that is counter to the Inspector General Act or DHS Management Directive?

Answer. The BCTF MOU places serious limitations on the independence of the OIG. First it requires that all allegations of DHS employee corruption, without exception, be referred to the BCTF. Second, it fails to address the authority within DHS to investigate allegations of criminal misconduct by DHS employees and the role of the OIG in oversight of DHS component internal affairs offices.

Inspectors General play a critical role in assuring transparent, honest, effective, and accountable government. Both the personal and organizational independence of OIG investigators is essential to maintaining the public trust in not only the work of the OIG, but also in the DHS workforce as a whole. The American public wants to know that Government employees are held accountable for their misconduct by an independent fact finder, such as the OIG.

The Inspector General Act of 1978, as amended, and the Homeland Security Act of 2002, as amended, establish a clear line of authority for investigating allegations of criminal misconduct by DHS employees. The statutes vest primary criminal investigative authority for employee misconduct with DHS OIG. Within DHS, Management Directive 0810.1 outlines the roles of the various offices of internal affairs with respect to support for the OIG, including investigation of noncriminal misconduct allegations.

In contrast, the BCTF MOU specifies that each participating DHS agency is an equal partner that shares overall responsibility for policy, operation, and direction of the BCTF; coordination of investigations; and for providing management and oversight of the BCTF. The San Diego BCTF includes the field operational elements of CBP and Border Patrol, in addition to CBP internal affairs and TSA's internal affairs. In fact, in the investigation of Border Patrol Agent Manzano, the FBI as-

signed a Border Patrol agent member of the BCTF to work as the co-case agent along with the FBI.

This shared management responsibility between DHS OIG and internal affairs units (and operational units) of other DHS components usurps the OIG's statutory responsibility for supervising, leading, and coordinating criminal investigations of DHS employees and interferes with our oversight responsibility with respect to component internal affairs units. Many aspects of the MOU interfere with the OIG's ability to investigate cases independently of the DHS component members of the BCTFs.

With respect to information sharing, the OIG and FBI have a mutual responsibility under the Attorney General's Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority to promptly notify one another upon initiation of any criminal investigation, a responsibility the OIG meets in a timely way. Within DHS, all allegations of criminal misconduct by employees must be referred to OIG. The MOU would require DHS participating agencies to provide the same information directly to the FBI. This duplication in reporting is not an efficient use of DHS or FBI resources, and opens the door for dual parallel investigations.

The MOU contains a provision under which the Executive Board, which is comprised of representatives of all participating agencies (in this case DHS components), who vote on whether or not the OIG could investigate an allegation unilaterally. Allowing DHS components to vote on whether and how the OIG pursues an investigation is contrary to the concept of statutory independence, and would result in the erosion of public confidence in any outcome.

Question. Describe the OIG's leadership role as it relates to the internal affairs division of each of the Department's agencies.

Answer. DHS OIG has strong working relationships with most offices of internal affairs within DHS. We communicate daily on allegations and ongoing cases, and routinely work collaboratively. DHS OIG has an established inspection process for reviewing the work of the internal affairs units at least once every 3 years. The inspections review compliance with investigative standards, personnel training and qualifications, and investigative case files in order to ensure that the work of the internal affairs units reflects the quality expected by DHS senior leadership, the Congress, and the public. Each inspection results in a written report and if recommendations are made for corrective actions or improvements, OIG follows up to confirm that the recommendations in fact have been implemented.

An OIG agent is assigned as a desk officer to each component internal affairs office and reviews allegations referred to OIG by that internal affairs office. OIG refers allegations that are purely administrative in nature back to the component, who then takes lead on the investigation. In certain instances of sensitive or significant matters, we exercise active oversight of a case referred back to the component and review the findings. DHS OIG also recently initiated a program to review case management statistics from each of the internal affairs units in order to reconcile OIG's case management records with those of the components, to track trends and patterns in allegations, and to ensure that components take appropriate action when misconduct is found.

Question. Should all internal affairs personnel work for the DHS OIG?

Answer. When the DHS was initially organized, it was done so on the basis of realignment of existing governmental resources. The premise was that the DHS would streamline operations by eliminating redundancies while increasing communication, information sharing, transparency, and accountability. Since that time, the component elements have inappropriately stratified operations by devoting personnel and resources that compete with, rather than compliment, the OIG. Although the internal affairs offices have an important mission to conduct noncriminal misconduct inquiries, pre-employment screening of applicants, and background investigations of employees and provide integrity and security briefings that help employees recognize corruption signs and dangers, transferring some number of experienced criminal investigators from the internal affairs offices to DHS OIG would allow OIG to more effectively address its workload growth resulting from increases in DHS component workforces. It is our belief that a realignment of these resources by transfer of the positions to the OIG would be responsible stewardship. Alternatively, funding for increased OIG staffing that reflects the growth within the DHS workforce is needed.

The Department was also founded with intent to forsake jurisdictional rivalries in favor of operational efficiency. Just as DHS presents one face at the border, the Homeland Security Act mandates one face when dealing with criminal allegations against departmental employees. The OIG, which has primary authority to investigate those criminal misconduct allegations, should be the single point of contact with regard to those allegations.

One of the most important factors in detecting, deterring, and discouraging corruption is employee awareness of where and how to report and their comfort in doing so. Centralizing complaint intake in the OIG, as a separate office from a complainant's agency of employment, would (1) provide DHS employees with increased assurance that their information will be treated confidentially and acted upon professionally; (2) eliminate redundancies in the reporting of allegations; and (3) ensure the timely reporting of employee complaints to the OIG hotline would more effectively direct resources to combat corruption and would promote better intelligence, trend analysis, and prioritization of investigative leads.

The OIG continues to work the vast majority of allegations of the most serious criminal misconduct and corruption, and has accounted for an overwhelming majority of all arrests and convictions of DHS employees since 2003. We believe that DHS's criminal investigative resources should be deployed accordingly.

U.S. CUSTOMS AND BORDER PROTECTION—CONTAINER SECURITY

Question. The 9/11 Act requires 100 percent of U.S.-bound maritime cargo to be scanned before departing to our ports. In testimony before the Congress last year, CBP Commissioner Bersin stated that only 4 percent to 5 percent of cargo is currently scanned. The act allows the Secretary to waive this 2012 requirement in a 2-year increment if conditions indicate this requirement cannot be met, and you have indicated that you will do so. However, even before you have officially waived these requirements, the budget request for fiscal year 2012—and the realities in this fiscal year—show significant reductions to the international cargo screening programs. Funds have been eliminated for Secure Freight pilots in all places except Pakistan and CBP has closed or is ceasing operations at many of the 58 Container Security Initiative (CSI) ports. In fiscal year 2009, there were 167 CBP officials located overseas at CSI ports. By the end of fiscal year 2010—and continuing today—the number of individuals has dropped to 86.

With overseas personnel for this effort essentially cut in one-half, how does this increase cargo security at the same time it appears that no real steps are being taken to meet a legislative mandate that the Department has known has been coming since September 2006—more than 4 years ago?

Much of this scanning will be handled domestically by the targeting center. However, the 2012 budget includes \$7.5 million to fund the implementation of two pilots to test the 100 percent scanning mandate. In fact, one of the proposed pilots appears to replicate the SFI model used in Pakistan in a different, high threat corridor—likely on the Arabian Peninsula.

What new information does the Department believe it can obtain by repeating the same project in a different location? How will this information be used to determine the best steps to meet the scanning requirement? What developments in scanning technology might lead DHS to decide to implement the overseas scanning requirement called for in the 9/11 Act?

Answer. Presently, and as required by the SAFE Port Act, DHS and other Federal partners are working collaboratively with the National Security Staff to develop a national-level strategy that will provide a unified vision that the U.S. Government sees for global supply chain security across air, land, and sea modes of transportation, which will also address the necessary level of cargo scanned to provide effective detection and deterrence. The administration anticipates completing this strategy development effort in 2011 and DHS remains confident that it will include guidance and additional details on how DHS, other Departments, and agencies will address the 100 percent cargo scanning provision.

Throughout this process, we will remain mindful of our need to properly balance security concerns with facilitating the flow of commerce. The President's fiscal year 2012 budget requests funding for CBP to conduct a cargo screening pilot to assess alternatives to the 100 percent maritime cargo scanning, enabling CBP to test alternatives to extend the zone of security beyond our physical borders, strengthen global supply chain security, and enhance CBP's multi-layered security strategy. CBP is in a unique position to work toward deterring malicious actors from exploiting the system, protecting infrastructure and embedding resilience in the system to aid in recovering from disruptions by virtue of having access to vast amounts of historical and transactional data from all modes of cargo shipments. This data includes the parties involved, trade routes and other information which can be used in assessing risk. Coupled with this is CBP's expertise in risk targeting that has been developed over the past decade. The proposed Supply Chain Security Pilot would include next generation targeting to employ predictive models to assess threats and detect anomalies in the supply chain; and the utilization of tools and technologies that are currently not in use at the National Targeting Center. For example, analysts will be

provided analytic tools that allow them to perform link analysis, commodity analysis, and entity resolution, along with visualization tools to represent vessel movements, geo-location of addresses, and social network diagrams.

CBP's multi-layered security strategy seeks to identify high-risk cargo as early as possible in the supply chain. The Trade Act of 2002 and its implementing regulations require industry to submit electronic manifest data to CBP 24 hours prior to the cargo being laden on a vessel destined for the United States. CBP's predeparture manifest data was enhanced further with the implementation of the Importer Security Filing and Additional Carrier requirements, commonly known as "10+2," which requires importers to provide specific information on their cargo prior to arrival in the United States. CBP also utilizes the Automated Targeting System (ATS) to screen advanced manifest data and assist CBP officers in identifying high-risk cargo. Upon screening, CBP can issue "Do Not Load" messages for shipments deemed high-risk until the risk can be mitigated or resolved.

Through the CSI, CBP works to identify and inspect high-risk cargo before it is laden on a vessel destined for the United States. As a result of new and improved technology and increased international partnerships, CBP is now able to conduct a greater portion of the CSI targeting from the National Targeting Center—Cargo (NTC-C)—increasing efficiency and reducing cost. As a result, in early fiscal year 2009, CSI began reducing the number of CBP officers deployed to foreign seaports. While there has been decrease in the staffing of CSI officers abroad, CSI has increased the staffing level at the NTC-C to support targeting functions in overseas ports. The decrease in the CSI staffing at foreign locations has not compromised the CSI mission because CBP has been able to accomplish the CSI mission more efficiently and in a more cost-effective manner through the increased staffing and resources at the NTC-C. The fiscal year 2012 budget continues to fund CSI at the same level.

CBP and DHS are committed to ensuring the security of the international supply chain and will work to support the global supply chain security strategy utilizing a risk-based, multi-layered approach across all modes of transit.

AIR CARGO SCREENING

Question. What specific steps is the Department taking to improve the screening of articles entering the United States via air? Is the Department taking steps to have shipping manifest requirements for air cargo more closely match the current ones for seaborne cargo? Can CBP ensure that all cargo information requiring a shippers' export declaration is provided to CBP within a reasonable security timeframe? If so, what is that timeframe? Does CBP currently have the ability to enforce a no-load decision or require additional screening for any U.S. bound air cargo?

Answer. Today, 100 percent of high-risk cargo on international flights bound for the United States is prohibited from being transported on passenger aircraft and goes through enhanced security procedures before being shipped on all cargo aircraft. DHS and the Transportation Security Administration (TSA) recently announced a proposed deadline of December 31, 2011 for industry to screen 100 percent of air cargo on international inbound passenger aircraft—2 years earlier than previously anticipated.

DHS is also working closely with industry and international partners to expedite the receipt of advanced cargo data for international flights to the United States prior to departure in order to identify and screen items based on risk and current intelligence before they are airborne. In December 2010, Customs and Border Protection (CBP), TSA, and the air cargo industry launched a new joint technology pilot project to enhance the sharing of electronic shipping information to improve the identification of high-risk shipments.

Further, in January, I announced a new partnership with the World Customs Organization to enlist other nations, international bodies, and the private sector in increasing the security of the global supply chain—outlining a series of new initiatives to make the system stronger, smarter and more resilient.

CBP exercises the same border authority over exports and imports and has the authority to inspect and detain goods and order their redelivery from any person, such as the carrier, in possession of the goods. CBP is currently collaborating with TSA to utilize their regulatory authority to have high-risk shipments screened prior to being laden at last port of departure.

Question. The Department has been working with industry to develop a process for receiving air cargo manifest information prior to departure. What is the status of this effort? When will the system be operational? What resources are required by CBP and TSA to develop and operate this system? Are funds requested in the fiscal year 2012 budget for this effort?

Answer. DHS is working closely with industry and international partners to expedite the receipt of advanced cargo data for international flights to the United States prior to departure in order to identify and screen items based on risk and current intelligence before they are airborne. In December 2010, CBP, TSA, and the air cargo industry launched a new joint technology pilot project (the Air Cargo Advance Screening Pilot) to enhance the sharing of electronic shipping information to improve the identification of high-risk shipments.

CBP and TSA have made significant progress on this pilot and expect to have the first phase—which focuses on the express consignment environment—fully operational in the late spring 2011. The passenger phase of the pilot is tentatively scheduled for implementation in early summer 2011.

CBP and TSA estimate that the total costs for the development and maintenance of the Air Cargo Advance Screening system and staffing through fiscal year 2012 will be approximately \$20 million. Funding is included within the CBP salaries and expenses appropriation, specifically in the Inspections, Trade and Travel, and Trusted Traveler Program PPAs, in the fiscal year 2012 budget request.

IMPACT OF CUSTOMS ENFORCEMENT ON THE SEAFOOD INDUSTRY

Question. When foreign producers send dumped or unfairly subsidized goods into our country, vigorous enforcement of our trade laws is the only way that American businesses can compete on a level playing field.

In Louisiana and the gulf region, the domestic shrimp industry is fighting a tough battle against unfairly dumped shrimp imports, and they won antidumping orders against shrimp from six countries in 2005.

Unfortunately, Customs is simply not doing enough to collect the dumping duties that importers owe to the Federal Government. Since 2005, for example, importers of shrimp from China have failed to pay more than \$58 million in dumping duties, some of which is supposed to be redistributed to injured shrimp producers here in the United States. Continued failure to collect these duties is fiscally irresponsible, and it further threatens a vulnerable gulf seafood industry that is struggling to recover from the impact of four major hurricanes and a devastating oil spill.

How can Customs improve its performance to ensure that our laws are fully enforced and that importers are held accountable for all of the duties they owe? Could we enforce duty payment requirements on individuals, rather than companies that often go bankrupt? Will you work with me to increase transparency so that domestic producers can track the enforcement actions Customs is undertaking against importers and the results of those actions?

Answer. Antidumping/Countervailing Duty (AD/CVD) Enforcement is a Priority Trade Issue (PTI) for Customs and Border Protection (CBP). CBP takes a concerted, systematic approach to detect and deter circumvention of the AD/CVD law, administer entries of AD/CVD merchandise, and to issue and collect bills for AD/CVD duties owed to the United States Government. CBP coordinates its AD/CVD enforcement activities through an intra-office AD/CVD PTI Working Group. CBP works closely with the U.S. Department of Commerce (Commerce), the administering authority for AD/CVD determinations under U.S. law, and U.S. Immigration and Customs Enforcement to enforce AD/CVD laws and regulations.

When CBP issues a bill for final AD/CVD duties, CBP makes every effort to collect all duties, taxes and fees legally due to the Government. However, some importers, or their agents, are unable to pay the final duties. In addition, at least two sureties issuing bonds covering substantial amounts of AD/CVD duties are currently in receivership, further complicating collection. Other importers are simply unwilling to pay, or no longer exist by the time CBP issues a bill. CBP pursues collection action against importers and sureties who are simply unwilling to pay. CBP's Revenue Division in the Office of Administration initiates an administrative collections process in order to recover past-due amounts from the importers and sureties. This process may include dunning letters and the suspension of the immediate delivery process, among other steps. Ultimately, those debts for which the Revenue Division's collections process is ineffective are referred to CBP's Office of Chief Counsel.

The Office of Chief Counsel pursues collection from both the importers and sureties, after completing a legal review of the underlying debt. Further, a review is done to determine if there is a viable importer (or available surety coverage) from which the debt may be recovered. In part, this is done through dunning letters, searches of electronic databases and internal systems, and pursuing available leads. In addition, CBP can assess civil penalties pursuant to 19 U.S.C. § 1592 against any party who, by fraud, gross negligence, or negligence submits a material false statement or omission on importation into the United States, including those cases in which a false statement or omission is made concerning the applicability of an anti-

dumping duty order to a particular entry. If administrative attempts to collect the debt are unsuccessful and a viable importer and/or surety can be found, the Office of Chief Counsel drafts a complaint and refers the matter to the Department of Justice for possible litigation in the Court of International Trade. If the Office of Chief Counsel is not successful in locating a viable entity to be pursued, the matter will be referred back to the Revenue Division for appropriate action. This may include referral to Immigration and Customs Enforcement for further investigation. If the debt is without legal merit or no viable entity can be located to pursue further collection action, CBP may ultimately be forced to write off the debt.

CBP has taken steps to specifically improve the collection of AD/CVD duties on shrimp imports and continues to explore statutory and nonstatutory changes to enhance bonding requirements. CBP is also actively pursuing collection of the balance of the open bills against delinquent importers and sureties.

ANTIDUMPING AUTHORITIES

Question. Please detail the legal process for antidumping activities (claims, investigations, collections, etc.) under the specific jurisdiction of U.S. Customs and Border Protection (CBP) from beginning of the process to final resolution.

What parts of this process are not under the control or jurisdiction of CBP? What roles do other U.S. agencies or departments play in this process and at what intervals? How long can the duty collection process take once a determination is made that a shipper has “dumped” goods adversely affecting a U.S. producer? What legal impediments, if any, prevent CBP from being able to use a portion of the fines it collects to cover the costs of increased investigations? Are all antidumping fines collected distributed to dumped-upon U.S. producers and/or companies?

Under current law, the U.S. Government assesses antidumping fines against a particular company or corporation. What prevents our Government from going after the individual owner(s) of the company or corporation? If there is a legal prohibition in doing so, what specific law prohibits it?

Answer. [Follows:]

Legal Process for Antidumping Activities

Once the Department of Commerce makes an affirmative determination in an Antidumping or Countervailing Duty (AD/CVD) investigation, it issues instructions to CBP specifically identifying the covered product and requiring the applicable AD/CVD duty rates for each foreign producer. An importer must indicate that its entry is covered by an antidumping duty or countervailing duty order on its entry forms and deposit the applicable cash deposit. Because the United States has a retrospective system for determining antidumping and countervailing duties, the liquidation of these entries is suspended until the Department of Commerce reaches a final decision of the rate of antidumping or countervailing duty. Thus, the amount deposited at the time of entry is only an estimate of what duties may ultimately be owed.

Once the Department of Commerce sends CBP liquidation instructions indicating the final rate of duty that is owed on these entries, CBP liquidates them in accordance with those instructions. If additional duties are owed, the importer must pay them at that time, with interest. Conversely, if the rate of duty decreased, the importer would receive a refund with any applicable interest. CBP's role in this process is purely ministerial as CBP implements the instructions received from the Department of Commerce.

An importer who disagrees with the imposition of antidumping or countervailing duties may file a protest with CBP that concerns a decision that was made by CBP at the time of entry (not the underlying determination by the Department of Commerce). Such a protest must be filed with the port within 180 days of liquidation.

If the protest includes a request for further review that satisfies 19 CFR 174.24, CBP headquarters reviews the protest and issues a binding decision. If the port improperly denied the request for further review, the protestant may seek to have the denial set aside. Alternatively, if a protest is denied, the protestant may file suit in the Court of International Trade, which is the U.S. Court with subject matter jurisdiction over these matters.

If the protestant does not seek judicial review of a denied protest (or if no protest was filed), CBP's Revenue Division in the Office of Administration initiates an administrative collections process in order to recover past-due amounts from the importers and sureties. This process may include dunning letters and the suspension of immediate delivery process, among other steps. Ultimately, those debts for which the Revenue Division's collections process is ineffective are referred to CBP's Office of Chief Counsel.

The Office of Chief Counsel pursues collection from both the importers and sureties, after completing a legal review of the underlying debt. Further, a review is

done to determine if there is a viable importer (or available surety coverage) from which the debt may be recovered. In part, this is done through dunning letters, searches of electronic databases and internal systems, and pursuing available leads. If administrative attempts to collect the debt are unsuccessful and a viable importer and/or surety can be found, the Office of Chief Counsel drafts a complaint and refers the matter to the Department of Justice for possible litigation in the Court of International Trade. If the Office of Chief Counsel is not successful in locating a viable entity to be pursued, the matter will be referred back to the Revenue Division for appropriate action. This may include referral to Immigration and Customs Enforcement for further investigation.

Parts of the Process Not Under the Control or Jurisdiction of CBP

CBP's role in administering the antidumping duty and countervailing duty orders is purely ministerial. The Department of Commerce establishes which products are covered by the orders and what the applicable duty rates are for foreign producers and U.S. importers. CBP is in charge of the collection of the cash deposits, reviewing entries to ensure that importers are properly reporting their goods as subject to an order and paying the correct rate of duty, and liquidating those entries and assessing the final duty rate that is owed for those entries. CBP does not, however, liquidate any entry subject to an antidumping duty or countervailing duty order until it receives specific instructions from Commerce indicating that it is appropriate to do so.

Roles Other U.S. Agencies Play

The U.S. Department of Commerce, the AD/CVD administering authority under U.S. law, and the U.S. International Trade Commission are responsible for investigating petitions alleging that goods being imported into the United States are dumped or subsidized. The Department of Commerce determines at what rate the goods are being dumped or subsidized and the International Trade Commission determines whether the U.S. industry has been injured or whether there is threat of injury resulting from the importation of these dumped or subsidized goods. If both agencies make affirmative preliminary determinations, the Department of Commerce issues instructions to CBP specifically identifying the covered product and the applicable required duty rates for each foreign producer. After both agencies make affirmative final determinations, the Department of Commerce publishes an antidumping duty order and/or countervailing duty order in the Federal Register. Thereafter, the Department of Commerce may conduct annual administrative reviews to determine the actual rate of dumping or subsidization of the previous year's entries.

Every 5 years, the Department of Commerce and the International Trade Commission conduct sunset reviews of AD/CVD orders to determine if a case should be continued or revoked, and the Department of Commerce instructs CBP accordingly if a case is revoked. The Department of Commerce also has other ad hoc proceedings that may result in instructions to CBP to begin or stop collecting AD/CVD duties on specified subcategories of merchandise or specific companies.

U.S. Immigration and Customs Enforcement (ICE) investigates criminal violations of AD/CVD laws. CBP works closely with ICE and regularly refers suspected criminal violations involving AD/CVD circumvention and fraud to ICE for investigation. In addition, CBP can assess civil penalties pursuant to 19 U.S.C. § 1592 against any party who, by fraud, gross negligence, or negligence, submits or aids and abets another in submitting a material false statement or omission on importation into the United States, including those cases in which a false statement or omission is made concerning the applicability of an antidumping duty order to a particular entry.

Steps in the Process Once a Determination Is Made

As soon as the Department of Commerce instructs CBP to collect estimated AD/CVD duties for a commodity from a specified country, CBP will collect these estimated duties upon entries of the merchandise into the United States. CBP will then hold these entries in suspension until the Department of Commerce instructs CBP to collect the final amount of duties due on these entries. CBP often does not receive these final liquidation instructions from the Department of Commerce for several years after the original entry of merchandise. CBP then works to take timely action to apply the liquidation instructions and bill the importers for the final AD/CVD duties due. Importers may legally protest the liquidation of an entry and delay paying a bill until the protest is decided. If a protest is denied, the protestant may file suit in the Court of International Trade.

Fines as a Funding Source

Generally speaking, fines must be deposited in the Treasury as miscellaneous receipts pursuant to 31 U.S.C. § 3302(b). Absent statutory authority, CBP's use of

these funds to cover the costs of investigations would constitute an improper augmentation of CBP's appropriations. Where goods are seized and forfeited for AD related violations, those proceeds from the sale of forfeited goods are deposited in the Treasury Forfeiture Fund and available for reimbursing costs of the investigations, among other uses.

Distribution of Fines

The "Continued Dumping and Subsidy Offset Act of 2000" was enacted on October 28, 2000, as part of the "Agriculture, Rural Development, Food and Drug Administration, and Related Agencies Appropriations Act". The act was repealed by section 7601(a) of the "Deficit Reduction Act of 2005", but remains in place for AD/CVD duties collected on entries made before October 1, 2007.

Money collected on an entry filed before October 1, 2007, will continue to be subject to the distribution procedures under former § 1675c. The duty on an entry is not available for distribution until the entry is liquidated pursuant to the direction of the Department of Commerce and the duty is collected and deposited into the special account; therefore, the distribution process will continue until all entries made before October 1, 2007 are liquidated and the duties are collected. As a result of the statutory constraints in the assessment of antidumping and countervailing duties, the distribution process will continue for an undetermined period; however, the amount of money available for distribution can be expected to diminish over time.

Enforcement on Individuals Rather Than Companies

The law makes it difficult to impose personal liability. While there is no express legal prohibition against taking collection action against individuals involved with corporate importers that incur dumping duty debts, most individuals involved with such debtor corporations are in other countries outside the jurisdiction of the United States, as is their valuable real and personal property.

However, CBP does have the authority to assess civil penalties against individual owners of particular companies or corporations. Pursuant to 19 U.S.C. § 1592, CBP is authorized to assess penalties and recover lost duties (including antidumping duties) against any party who, by fraud, gross negligence, or negligence, enters or introduces, or attempts to enter or introduce, any merchandise into the commerce of the United States by means of a false statement or omission, or aids or abets another person to do so. See 19 U.S.C. § 1592(a)–(d). CBP may exercise this authority in cases in which a false statement or omission is made on an entry involving merchandise subject to an antidumping duty order.

IMPROVED ANTIDUMPING REVENUE COLLECTIONS

Question. In March 2008, the Government Accountability Office (GAO) reported that, as of September 2007, CBP has been unable to collect more than \$600 million owed in antidumping and countervailing duties imposed to remedy injurious unfair foreign trade practices. These include duties imposed on products exported to the United States at unfairly low prices (i.e., dumped) and duties on products exported to the United States that were subsidized by foreign governments. In addition to the substantial amount of lost revenue, the uncollected duties cause concern that the U.S. Government has not fully remedied the unfair trade practices.

Since 2005, the GAO has reported several times on the U.S. Government's inability to collect substantial amounts of antidumping and countervailing duties and, in 2008, proposed a variety of options for improving the system for collecting these duties. Two key components of the antidumping and countervailing duty system have received particular attention. One is its retrospective nature, which means that—though importers pay estimated duties at the time of importation—final duties are not assessed until after products enter the country. Another component is the "new shipper" review process that allows new manufacturers or exporters to petition for their own separate antidumping and countervailing duty rate. Despite other efforts by the Congress and CBP, these components of the system have not been addressed and the collection of antidumping and countervailing duties remains a problem.

The March 2008, GAO report identified several options for the Congress to consider for improving the collection of antidumping and countervailing duties. And by adjusting features of the antidumping or countervailing duty system that create the risk that companies can evade paying duties, the Congress could further protect Government revenue, while also minimizing incentives for companies to pursue unfair trade practices. These options included eliminating the retrospective component of the U.S. antidumping and countervailing duty system and adjusting requirements for new shipper reviews.

What specific laws does CBP recommend should be changed or amended to enhance CBP's antidumping investigations and increase antidumping collections? Can

CBP take administrative actions to improve antidumping collections in the absence of legislation? In the absence of changes in legislative authorities to existing laws and practices, can CBP do more to collect and distribute antidumping receipts to injured U.S. businesses if it was provided with additional resources? If so, what resources would be required and what more could be achieved?

Answer. CBP has a longstanding administrative collection process that employs all of the authority available to CBP. CBP makes every effort to collect all duties, taxes and fees legally due to the Government.

In appendix V of the March 2008 GAO Report, DHS commented that of the options identified by the GAO to improve the collection of AD/CVD duties, the first option CBP preferred for addressing uncollected AD/CVD duties would be for the U.S. Congress to change U.S. law to eliminate the retrospective component of the U.S. AD/CVD system and make the U.S. AD/CVD system prospective. DHS noted that a prospective AD/CVD system would alleviate the collection issues faced by CBP since the amount of duty assessed at entry would be the final amount owed. This would also substantially alleviate the administrative burden on CBP resources associated with a retrospective system, and allow CBP resources to more fully focus on AD/CVD enforcement issues, such as circumvention of the AD/CVD law. In this appendix to the March 2008 GAO Report, DHS also commented that the majority of the other options identified by the GAO to improve the collection of AD/CVD duties would perpetuate and exacerbate the shortcomings of the U.S. retrospective system.

JONES ACT ENFORCEMENT

Question. CBP is charged with enforcing our Nation's cabotage laws, including the Jones Act, which requires that any goods transported by water between two coastwise points in the United States must be carried on ships that are built in America and crewed by Americans. This law promotes our economic and national security by ensuring the existence of a robust merchant marine fleet.

The Outer Continental Shelf Lands Act of 1974 extended Jones Act requirements to offshore points within the Exclusive Economic Zone of the United States. It is therefore imperative that CBP have both the resources and the authorities it needs to enforce the Jones Act offshore, particularly in the Gulf of Mexico, where more than 25 percent of America's domestic energy production occurs.

Does CBP have the resources, authorities, and information it needs to investigate alleged Jones Act violations offshore? How is CBP partnering with the Offshore Supply Vessel (OSV) industry, which supports offshore energy facilities and operations, to carry out its enforcement mission?

Answer. Yes, CBP has the resources, authorities, and information needed to take appropriate action for alleged Jones Act violations committed offshore.

AIR AND MARINE

Question. What are the operational impacts on performing CBP's mission of the CBP plan to retire 18 single-engine, fixed wing aircraft in fiscal year 2011?

Answer. CBP is scheduled to retire 16 single-engine, fixed wing aircraft, 15 PA-18s and 1 C-172 in fiscal year-2011. The decision to retire these aircraft was based on their advanced age and the desire to operate more efficient, effective, and capably equipped aircraft. The PA-18 and C-172 have limited capability to fly low-level missions over hazardous terrain during the day and virtually no capability for operational missions at night. Recently purchased light enforcement helicopters (AS-350) are equipped with sophisticated sensors and are considerably better suited to perform the variety of required law enforcement missions supported by OAM.

WHEN WILL WE KNOW THE BORDER IS SECURE?

Question. Debates have raged in the Congress and around the country over how secure our border is—especially our border with Mexico. Many people assert that they will not support immigration reform until they are confident the borders are “secure”. I look forward to visiting the border this spring to see what has been accomplished and to listen to the men and women who work to secure the border about what more needs to be done.

But there appears to be no consensus on what constitutes a secure border. As I understand it, the Border Patrol for years has used metrics such as “effective control” or “less monitored” in defining border security. Approximately 657 miles of fencing and vehicle barriers have been constructed along the Southwest Border to date. And as of June 30, 2010, the Border Patrol determined that 774 miles of that border were under “effective control”.

In testimony earlier this year, you stated “the term ‘operational control’ is a very narrow term of art, and it does not reflect the infrastructure and technology and all the other things that happen at the border”. I would assume that 657 miles of fencing would certainly contribute to control of the border.

Are you modifying the metrics used to define “border control”? Do you believe our borders are secure? Which agency or entity determines where, how much, and what kind of tactical infrastructure is required to obtain control of our borders? What is the required number of miles of fencing to be constructed mandated by the Secure Fence Act, as amended?

Answer. The “Operational Control” measure did not accurately represent the Border Patrol’s significant investments in personnel, technology, and resources or the efforts of other DHS Components who are engaged in border security such as U.S. Immigration and Customs Enforcement and the U.S. Coast Guard. The Border Patrol is currently taking steps to replace this outdated measure with performance metrics that more accurately depict the state of border security.

This administration has made unprecedented investments in border security and on every metric that measures progress, we’re heading in the right direction. Apprehensions are down and seizures—across the board—are up.

The types, amount and location of tactical infrastructure are determined through a combination of the operational assessment made by Border Patrol agents conducting daily operations in the field, available funding, and an overall determination of current operational priorities.

To date, DHS/CBP has constructed a total of 649 miles out of nearly 652 miles required by the Congress. The fence mileage language of the Secure Fence Act, as amended, is currently the subject of pending litigation (*United States v. The State of Arizona*; United States District Court, District of Arizona; Case No. 10-cv-01413).

BORDER PATROL AGENTS

Question. Your budget request supports funding to sustain the 21,370 Border Patrol agents which CBP intends to hire by the end of this fiscal year. This number reflects the additional 1,000 agents the Congress funded as part of the Fiscal Year 2010 Emergency Border Security Supplemental Appropriations Act enacted last August. No new agents, however, are requested in the President’s budget.

Are 21,370 Border Patrol agents the right number of agents needed to protect our borders? What happens when the 1,200 National Guardsmen and women currently assisting our border agencies along the Southwest Border leave as planned this summer?

Answer. The fiscal year 2012 budget request supports 21,370 Border Patrol agents and 21,186 CBP officers—the largest deployment of law enforcement officers to the front line in the agency’s history. The request annualizes positions supported by the fiscal year 2010 SWB Supplemental, including 1,000 new Border Patrol agents and 250 new CBP officers. Additional funding is provided to support 300 more CBP officers and canine assets at ports of entry. The request also supports the mobile response surge teams created with the Supplemental funding to respond rapidly to emergent situations without depleting Border Patrol staffing from other locations. The 1,200 National Guard deployed to the Southwest Border have been contributing additional capabilities and capacity to assist law enforcement agencies including providing intelligence, surveillance, reconnaissance, and counternarcotics enforcement support as CBP hires and deploys the 1,000 BP agents included in the Southwest Border supplemental.

IMPROVING THE ENTRY PROCESS FOR VISITORS TO THE UNITED STATES

Question. In your statement, you say the second Homeland Security mission is to secure the Nation’s borders “to prevent illegal activity while facilitating lawful travel and trade.” We want to welcome visitors to the United States, but I frequently hear from constituents who travel internationally that the entry process coming into this country is lengthy and daunting. It often takes hours for passengers to be processed once arriving at an airport. There are long lines, not all lanes are open and staffed, and the information provided to arriving passengers is often confusing. I understand that your Department has initiated a few programs to try and address some of these symptoms, such as the Model Ports of Entry program and the Global Entry Program.

Your budget proposes funding to add more than 300 new Customs and Border Protection officers to staff newly opened or expanded land border ports. What is being done to make the entry process for visitors and U.S. citizens more welcoming without degrading security? Please explain how these existing programs, and others, have reduced wait times and made the process more welcoming for travelers. How

much money has been directed to these improved entry programs for each of fiscal years 2008–2011, and how much is requested for these and other programs for 2012?

The Department has implemented a number of the recommendations proposed by the Secure Borders and Open Doors Advisory Committee (SBODAC)—such as the International Registered Traveler program and those programs listed above. In an October, 28, 2008, letter to now former Secretaries of State and Homeland Security, Rice and Chertoff, respectively, the SBODAC urged that additional actions recommended in the Committee’s January 2008 report also be implemented.

Has the Department implemented any additional recommendations of that Committee since 2008? If so, please describe them. If not, please explain why it has not?

One of the frequent complaints made by visitors to the United States, especially in the air environment, concerns the way they are treated by CBP officers upon arrival at the airport. The visitors are often tired and there may be language barriers, but unfortunately what makes the media reports is that the CBP officers are brusque and treat the visitor as if he or she is guilty while performing the entry inspection. Understanding that the CBP officers’ primary duty is security and ensuring that the individual before them is eligible for entry into the country, the officer is also the first impression the traveler has of America and Americans.

Please describe the training CBPOs are provided regarding “welcoming” visitors as they are being processed. Are aspects of courtesy and customer service, in addition to security, stressed as part of their training? Are they instructed to greet the visitor with a statement such as “Welcome to the United States” as the traveler approaches the inspection kiosk? If not, are there reasons why the officer should not be provided such instruction?

Answer. [Follows:]

Programs To Welcome Travelers

CBP developed the Model Ports Initiative in partnership with industry stakeholders, launching the pilot program in 2007 at Washington/Dulles and Houston International Airports. The program expanded to 18 additional model ports in 2008, including Atlanta, Boston, Dallas/Fort Worth, Chicago, Detroit, Fort Lauderdale, Honolulu, Las Vegas, Los Angeles, Miami, Newark, New York (JFK), Orlando, Philadelphia, Sanford (FL), San Juan, San Francisco, and Seattle airports.

The Model Ports Initiative is the key component of efforts to strengthen border security through advanced technologies and procedures while providing a more welcoming experience, reduced wait times and better customer service. CBP has increased staffing and professional training at ports of entry, installed new bilingual signage, updated the travel section of its public Web site and introduced a variety of trusted traveler programs, such as Global Entry, to expedite entry into the country.

The Passenger Service Manager (PSM) program continues to be an important focus of the Model Ports Initiative to welcome travelers, provide appropriate assistance, and explain CBP procedures in order to minimize wait times.

All Model Ports signage have been completed and delivered. These signs inform travelers of the CBP mission, pledge to treat people with respect and provide clear directions to travelers to minimize delays.

The audio and video displays which run the updated “Welcome to the United States” video, and a 1-minute Global Entry promotional video, have been installed at all locations. These videos provide a welcome experience to arriving travelers, inform them of CBP procedures to reduce delays and burdens for legitimate travelers, and promote the Global Entry program to reduce wait times. Global Entry, one of CBP’s trusted traveler programs designed to expedite clearance of preapproved, low-risk, recurrently vetted air travelers entering the United States, is available at all 20 model ports. This program utilizes automated kiosks that scan members’ fingerprints to bypass the regular passport control queues (unless chosen for a selective or random secondary referral).

In order to make meaningful and responsive changes to the arrivals processes where practical, and apply resources where needed, CBP is conducting a traveler satisfaction survey in the spring of 2011 to benchmark passenger satisfaction at the 20 model ports of entry.

Working with the Department of State, CBP improved the diplomatic arrival processes and has ensured that every model airport and terminal has dedicated diplomatic processing lanes to welcome and expedite the entry of foreign dignitaries and diplomats. This represents at least 36 dedicated passport primary lanes at the Nation’s airports.

As part of the emergency border security appropriations in fiscal year 2008 CBP received \$40 million for the Model Ports of Entry program, which included 235 addi-

tional CBP officers, and funding for overtime, video equipment, and services at the model ports. CBP spent \$22,900,000 to hire the additional staff, \$2.1 million for training, \$8.5 million for equipment and \$6.5 million for overtime at the model ports. Excluding the continuing resources used to maintain the additional CBP officers, CBP spent approximately \$692,000 for Model Ports program in fiscal year 2009 and an additional \$250,000 in fiscal year 2010. For fiscal year 2011 and fiscal year 2012 there is an annualization in the base for the position costs as well as \$1.3 million for nonpersonnel costs for Model Ports.

For Global Entry, CBP spent approximately \$800,000 in fiscal year 2009 and \$1.7 million in fiscal year 2010, including for kiosks, IT, and video. In addition, CBP spent \$2.1 million for fiscal year 2008–2009 for fingerprinting applicants for all Trusted Traveler programs. The cost for fingerprinting for Trusted Traveler programs was \$4.1 million in fiscal year 2010, and CBP anticipates it will cost approximately \$5 million in fiscal year 2011 and fiscal year 2012. Although CBP recovers a portion of the costs in the fees for this program, it does not recover the full amount.

In November 2009, CBP issued a Notice of Proposed Rulemaking that established an application fee for participants in the Global Entry program. This fee was authorized to recover the full cost of processing an application. The chart below shows the collections from Global Entry applicants in fiscal year 2009 and fiscal year 2010 and projected revenues in fiscal year 2011 and fiscal year 2012.

- Fiscal year 2009 actual: \$1,993,546.
- Fiscal year 2010 actual: \$4,989,847.
- Fiscal year 2011 (estimate): \$5,099,624.
- Fiscal year 2012 (estimate): \$5,201,616.

Secure Border and Open Doors Advisory Committee (SBODAC)

The Secure Border and Open Doors Advisory Committee (SBODAC) was an ad hoc subcommittee of the Homeland Security Advisory Council (HSAC), an advisory body to the Secretary of Homeland Security that was established under the provisions of the Federal Advisory Committee Act (5 U.S.C. Appendix). The SBODAC prepared and provided reports to the HSAC on important issues that affect our country's ability to attract and treat visitors in a secure and welcoming manner, completing its work on December 1, 2008. The HSAC recommended, and DHS is continuing to implement, recommendations from the HSAC's final report, including:

Visa Policy and Processing

- The Departments of Homeland Security and State should fix a longstanding obstacle to reliable business traveler entry from Canada by increasing visa training for CBP officers and establishing an optional pretravel approval process for qualified Canadian business visa applicants.

Status.—The NEXUS program allows prescreened travelers expedited processing by United States (Customs and Border Protection) and Canadian (Canada Border Services Agency) officials at dedicated processing lanes at designated Northern Border ports of entry, at NEXUS kiosks at Canadian Preclearance airports, and at marine reporting locations. Individuals approved to participate in NEXUS receive an identification card.

- The Departments of Homeland Security and State should continue to improve the reliability, responsiveness, and integration of processes to ensure that visa-related errors in the consular and port-of-entry systems are corrected in a timely and effective manner.

Status.—DHS has a strong relationship with the Department of State and the two agencies continue to work together to improve the systems that transmit and receive visa data. Errors in transmission are quickly detected and resolved through interagency technical working groups.

Ports of Entry

- Airports.*—The Department of Homeland Security should establish a pilot program for International Registered Travelers as soon as possible and promptly expand the program to the top 20 international airports.

Status.—CBP has established and currently operates such an international trusted traveler pilot program: Global Entry. Global Entry began operations on June 6, 2008 at 3 airports, and has since been expanded by CBP to the top 20 U.S. airports. Additionally, CBP has implemented arrangements with the Governments of the Netherlands and Mexico to expand eligibility for Global Entry to qualified citizens of those countries who meet program requirements, as well provided access to Global Entry benefits to Canadians who are members of the NEXUS trusted traveler program.

CBP has enrolled more than 120,000 participants, as well as 390,000 persons able to use Global Entry as members of NEXUS and 89,000 as members of Secure Electronic Network for Travelers Rapid Inspection (SENTRI).

DHS conducted a statistical analysis of wait times for Global Entry pilot participants, which indicated that Global Entry reduces a passenger's wait time by up to 70 percent—or an estimated 7 minutes on average. Wait time is defined as the time interval between the arrival of the aircraft (the block time) and the processing of the passenger by a CBP officer at the primary booth, less the walk time.

—*Airports.*—The Departments of Homeland Security and State should accelerate and expand the Model Ports program and fully include TSA to eliminate redundant rescreening of baggage and passengers.

Status.—CBP continues to expand the Model Ports program, which provides a more welcoming arrival experience at the 20 top U.S. airports for international arrival. Since the SBODAC report was issued, the Model Ports program has launched and expanded several initiatives. Improved signage communicates clear, accessible instructions to incoming passengers as they enter the CBP area. A new, improved airport wait-time monitoring system gives the traveling public better information on expected wait times upon arriving at the airport. CBP has deployed additional officers at the Model Ports, as well as provided enhanced professionalism training as part of the officer academy and field refresher training curricula. CBP has deployed Passenger Service Managers to greet travelers and serve as a point of contact at the airport to deal with passenger complaints and concerns. CBP has completed deployment of audio and video equipment that displays a welcome video donated by Walt Disney Parks and Resorts called “Welcome: Portraits of America” and a CBP instructional video called “Welcome to the United States: Simple as 1, 2, 3.” CBP continues to collaborate with its partners in the private sector, municipalities, and the Federal Government to improve the entire arrivals process, including making the queuing area more welcoming, improving wait-times and baggage delivery and being available to address travelers’ questions and concerns.

—*Airports.*—The Department of Homeland Security should continue to improve security performance while reducing the average amount of time U.S. Customs and Border Protection officers spend with each traveler to less than pre-September 11 levels and staff ports of entry sufficiently to complete primary inspection of foreign passengers in less than 30 minutes by December 2009.

Status.—CBP is committed to processing incoming travelers as efficiently as possible consistent with meeting the Nation’s security needs. In the first quarter of fiscal year 2011, the vast majority of air passengers admitted into the United States experienced wait times of less than 30 minutes at the CBP inspection area.

—*Land Borders.*—CBP should increase the effectiveness of NEXUS, SENTRI, and FAST trusted traveler programs.

Status.—Our NEXUS, Secure Electronic Network for Travelers Rapid Inspection (SENTRI), and Fast and Secure Trade (FAST) trusted traveler programs are very effective, and enrollment has been growing. CBP has increased effectiveness by harmonizing enrollment infrastructure, as well as expanding membership benefits. All programs use the Global Enrollment System, as well as harmonized requirements for enrollment data, vetting, and disqualifying offenses. TSA now recognizes trusted traveler identity documents at domestic airport checkpoints. NEXUS and SENTRI members can automatically use Global Entry kiosks, where available, when entering the United States by air.

—*Land Borders.*—The Departments should implement the Western Hemisphere Travel Initiative (WHTI) and US-VISIT on the land border without degrading the travel experience.

Status.—DHS implemented WHTI at the land ports of entry in June 2009. Compliance with document requirements is high, and many individuals (almost 9 million so far) are obtaining documents enhanced by radio frequency identification (RFID) technology that increases the efficiency of the inspection process. This technology allows law enforcement queries 60 percent faster than relying on manual entry and 20 percent faster than “swiping” the document’s machine readable zone. New license plate readers have been installed, reducing erroneous reads and saving 10 million manual corrections per year. WHTI also supports lane flow optimization that can adapt to traffic patterns and port needs, is installing new signage to help travelers advance more smoothly, and is instituting “ready lanes” used by travelers with RFID-enabled documents to further facilitate border crossing.

Implementation of WHTI has made travel more secure by limiting the number of documents that can be presented at the port of entry and allowing CBP to conduct law enforcement queries on an increased number of higher risk travelers.

—The Department of Homeland Security should assess its traveler screening programs within 9 months to share and harmonize best practices and technology among agencies.

Status.—DHS continually reviews its traveler screening programs to ensure that the business processes and underlying systems support the mission needs and to pursue harmonization. In July 2006, DHS established the Screening Coordination Office (SCO) in the Office of Policy to identify and promote best practices and ensure a coordinated approach to investments in screening programs.

Training

CBP officers receive extensive training on professionalism and cultural diversity awareness, including appropriately greeting travelers, to ensure they interact with the traveling public with courtesy and respect. This begins as soon as new hires enter on duty and continues throughout their career. Incumbent officers and supervisory officers are reminded of these core values through Web-based training, classroom training, and musters to ensure personnel treat travelers with dignity and respect. Professionalism is also a performance evaluation measure for the officer position. Officers are instructed through training and musters to be courteous to the traveler, emphasizing establishment of rapport as a key interview and observation techniques tools for the detection of admissibility, counter-terrorism, and/or smuggling issues.

OVERTIME PAY REFORM

Question. The budget includes a placeholder for a legislative proposal to reform overtime pay for CBP. This is an authorization issue which must first be addressed by the appropriate authorizing committees.

Please provide a copy of the legislative proposal. Please provide copies of any formal requests to the authorizing committees to take action on this proposal. What is the long-term impact on agents of implementing this proposal? Will implementation of this proposal have cascading effects on future pay costs for agents or other CBP or DHS personnel in the out-years and have any impacts been considering in formulating this proposal? What cuts to the budget, if any, would you propose be made if overtime pay reform is not enacted?

Answer. The administration continues to work to develop the legislative proposal referenced in the President's budget request for fiscal year 2012 regarding CBP's personnel system. The reforms being proposed eliminate redundancies and other inefficiencies that resulted from merging three different workforces from three different legacy agencies and make it easier for CBP employees to take positions across the agency, ensuring that CBP makes the most efficient use of taxpayer dollars. DHS will provide the legislative proposal as soon as it is finalized.

BORDER PATROL CONSTRUCTION

Question. Are any funds requested in the budget for construction of new Border Patrol facilities, including checkpoints?

Answer. Fiscal year 2012 budget does not include resources for the construction of new facilities.

ADVANCED TRAINING CENTER

Question. How much is requested in the President's budget for training activities and training operations at the Advanced Training Center (ATC) in fiscal year 2012? Also, what is the staffing target for the ATC?

Answer. The fiscal year 2012 projected programmatic expenses for the ATC total \$47,663,341, which includes salaries and benefits and other programmatic expenses. The fiscal year 2012 staffing target is 157 positions.

AIR AND MARINE

Question. What specific types of aircraft and in what quantities are proposed to be procured by this budget request? Will all of the previously funded Unmanned Aircraft Systems (UASs) be fully outfitted with prior year funds and the funds requested in this budget? If not, what additional funds are required to make these systems fully operational?

Answer. The fiscal year 2012 proposed budget provides funding for two P-3 replacement wing sets in continuation of the P-3 Service Life Extension Program, six

AS-350 light enforcement helicopters, and to induct two UH60 Black Hawk helicopters in the A to L model conversion program. The two replacement wing sets funded in the fiscal year 2012 budget will complete the acquisition objective for 14 new sets for the 16 P-3 aircraft in the OAM fleet.

In addition, funds provided in the fiscal year 2010 Southwest Border supplemental are being used to acquire two additional UASs. The fiscal year 2012 budget request includes \$4 million to complete this acquisition. The first of the two Predator B UASs purchased with the supplemental funding should be delivered in October 2011.

UNITED STATES IMMIGRATION AND CUSTOMS ENFORCEMENT—VIOLENCE IN MEXICO

Question. The tragic and senseless murder of Immigration and Customs Enforcement Special Agent Zapata and the wounding of his partner Special Agent Avila on February 15, brought to light the fact that our agents are prohibited from carrying service weapons for their own defense. More than 33,400 Mexican citizens have died during the Mexican Government's admirable campaign against the drug trafficking organizations. It is our Government's policy to assist the Mexicans in this effort. But as we put United States personnel in Mexico to help that government, our people can become targets.

Why are our special agents and other personnel not allowed to carry weapons to protect themselves? Is this prohibition limited to ICE personnel, all Homeland Security personnel, or does it apply to all American Government law enforcement working with Mexican authorities in that country? I want to ensure that the same rules apply to all U.S. law enforcement. Do ICE special agents receive hazardous duty pay during their assignment in Mexico, the way that other United States law enforcement do when working in war zones such as Iraq and Afghanistan? Are special agents permitted to turn down overseas assignments such as these if they fear for their personal safety? What has been the special agent force reaction to serving in Mexico since the Zapata killing? Media reports claim that the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) estimates that 90 percent of the guns seized by the Mexican Government are eventually found to have been purchased in the United States. Is this a valid statistic? Does this represent all guns seized by the Mexican Government, or only the portion of seized guns United States officials are given access to? Are guns used by the drug cartels found to come from countries other than the United States? If so, from which countries are these guns coming?

Answer. Sadly, the tragedy you mention involving two special agents assigned to ICE's attaché office in Mexico City is a stark reminder of the dangers confronted and the sacrifices made every day by our Nation's law enforcement officers. Special Agent Jaime J. Zapata lost his life and Special Agent Victor Avila, Jr. was critically injured in service of our country. While these remain ongoing investigations, Mexican authorities have apprehended some of the individuals involved in the murder of ICE Agent Jaime Zapata. We will continue to assist the ongoing Mexican investigation with every resource at our disposal and to ensure that all those responsible for these murders face justice. In coordination with the Departments of State and Justice, we have announced a reward of up to \$5 million for information leading to the arrest and/or conviction of additional individuals responsible for the murder of Special Agent Jaime Zapata and the attempted murder of Special Agent Victor Avila. In addition, the FBI, in conjunction with ICE, has established a 24-hour tip line based in the United States to process the information.

It is our understanding that, in general, the Department of State (DOS), through the Chief of Mission (Ambassador), determines whether U.S. law enforcement officers may carry firearms overseas and under what conditions, in accordance with 22 U.S.C. § 3927 and host country laws and agreements, and that the Chief of Mission's authority would apply to all American law enforcement personnel.

While DOS is the authority on specific questions regarding their policy for hazardous duty pay in war zones, ICE personnel do receive the same hardship pay as other United States civilian personnel in Mexico. However, ICE personnel only receive danger pay in certain locations in Mexico (Tijuana, Ciudad Juarez, and Monterrey). Location based danger pay varies among the United States law enforcement agencies with personnel in Mexico due to the statutory authority for danger pay allowance, which is set forth in 5 U.S.C. § 5928. Currently, there are locations in Mexico, specifically Mexico City and Hermosillo, where Drug Enforcement Administration (DEA) and the Federal Bureau of Investigation (FBI) personnel receive danger pay and ICE personnel do not. The following table shows the current rates established by DOS of hardship pay and danger pay received by personnel assigned to Mexico:

Location	Post (hardship) differential percent of basic compensation	Danger pay percent of basic compensation
Ciudad Juarez, Chihuahua, Mexico	10	20
Mexico City, D.F., Mexico	15
Tijuana, Mexico	5	15
Hermosillo, Mexico	15
Monterrey, Mexico	5	20

All ICE overseas positions are considered voluntary. ICE posts announcements to advertise overseas positions and interested personnel respond to the announcements and undergo the necessary application procedures. Applicants may withdraw from the selection process at any time.

In response to Special Agent Zapata's murder, ICE has sent 29 special agents, 1 criminal research specialist, 2 victim/witness counselors, and 2 technical enforcement officers on temporary duty assignments to Mexico City and Monterrey to directly assist the FBI and the Government of Mexico in the investigation. ICE personnel in Mexico also implemented rigorous security measures designed to protect ICE employees and their families. Additionally, ICE met with other Federal, State, and local law enforcement agencies in the United States to coordinate a domestic investigative and law enforcement response against the organization believed to be responsible for the attack, and its criminal associates.

In regard to the ATF statistic, we respectfully defer to the ATF.

REMOVAL STATISTICS

Question. Some have called the administration's claim of achieving a "record" number of deportations for fiscal year 2010 inflated, citing findings from the Center for Investigative Reporting. Those findings allege that ICE included 19,000 immigrants who departed the previous year, and 6,500 from a Mexican repatriation program that ran 5 weeks longer than it had previously. They also claim that nearly 65,000 of the deportations were voluntary and that the agency pushed the voluntary-departure option in deportation figures just long enough to make its annual goal for removals.

Are these allegations accurate? Please provide the statistics for each of these categories for fiscal years 2008–2010. Also, please provide the metrics used by the administration to measure increased rates of removal for the same 3 fiscal years.

Answer. In fiscal year 2010, ICE set a record for overall removals of illegal aliens, with more than 392,000 removals nationwide. One-half of those removed—more than 195,000—were convicted criminals. The fiscal year 2010 statistics represent increases of more than 23,000 removals overall and 81,000 criminal removals compared to fiscal year 2008—a more than 70 percent increase in removal of criminal aliens from the previous administration.

When compared to fiscal year 2009, ICE returned 6,527 more aliens through fiscal year 2010's Mexican Interior Repatriation Program (MIRP). Since 2008, MIRP statistics have been included in ICE's overall removal numbers. MIRP is a seasonal program designed to run during the summer months; however, the actual dates of the program fluctuate each year dependent upon completion of annual negotiations between the Department of Homeland Security and the Government of Mexico, and the identification of requisite funding.

Please see the charts below which address statistics for removal categories in fiscal year 2008 through fiscal year 2010 and metrics used by the administration to measure increased rates of removal for fiscal year 2008 through fiscal year 2010.

	Fiscal year 2008	Fiscal year 2009	Fiscal year 2010
BREAKDOWN OF TOTAL ICE REMOVALS/RETURNS			
Actual Fiscal Year Removals/Returns	\$369,221	\$387,790	\$373,440
Case Closure Lag ¹	(²)	2,044	19,422
Total ICE Removals/Returns	369,221	389,834	392,862

HISTORICAL STATISTICS FOR VOLUNTARY RETURNS AND THE MEXICAN INTERIOR REPATRIATION PROGRAM
(Voluntary returns and Mexican repatriation program removals/returns are a subset of the actual fiscal year removals/returns included in the previous chart.)

Voluntary Returns	84,466	70,211	64,876
Mexican Interior Repatriation Program Removals/Returns	18,464	10,560	23,384

Fiscal years 2008–2010 data is historical and remains static. Fiscal year 2010 data is as of 10/05/10.

¹ Fiscal year data lag/case closure lag is defined as the physical removal of an alien that occurs in a given fiscal year but the information is not recorded in EARM nor is the case closed in EARM during that fiscal year. Because the data in EARM is locked at the end of each fiscal year, the removal is recorded for the month the case was closed but reported in the following fiscal year removals.

² Not available.

SECURE COMMUNITIES

Question. There is confusion as to whether ICE considers local participation in Secure Communities mandatory. What is your policy? If it is not mandatory, on what basis do you assert that all communities will be enrolled by 2013?

Answer. There has been confusion as to what is meant by “opting out” in the context of Secure Communities and whether “opting out” is possible. Once a State signs an agreement with ICE to implement Secure Communities, it is mandatory that all fingerprints collected by law enforcement agencies in that State and submitted to the FBI be shared with ICE. Once Secure Communities is activated in a jurisdiction, the fingerprints that jurisdiction submits to the Department of Justice’s biometric system to check for criminal history records are automatically sent to DHS’s biometric system to check against its immigration and law enforcement records. The United States Government has determined that a jurisdiction cannot choose to have the fingerprints it submits to the Federal Government processed only for criminal history checks. Nor can a jurisdiction demand that the identifications that result from DHS’s processing of the fingerprints be withheld from local ICE field offices in that jurisdiction. The ICE local field office, and not the State or local law enforcement agency, determines what immigration enforcement action, if any, is appropriate.

A jurisdiction may, however, choose not to receive the identifications that result from processing the fingerprints through DHS’s biometric system. A jurisdiction’s decision not to receive this information does not affect whether the local ICE field office in that jurisdiction will or will not take enforcement action based on those identifications. In that sense, jurisdictions may “opt out” of receiving the results of Secure Communities biometrics checks.

DETENTION REFORM

Question. The Department has made impressive gains in detaining and removing criminal aliens who pose a danger to people lawfully present in the United States. I understand your budget request provides sufficient funds to maintain the mandated level of 33,400 detention beds. And the request also includes an increase of \$6.5 million for the alternatives to detention program to expand the number of individuals who need to be monitored but not necessarily held in custody prior to resolution of their immigration status. But while the administration has claimed it is pursuing detention reform, your budget for this activity is essentially flat.

How can you achieve improvements in meeting your third mission goal—enforcing and administering our immigration laws—if your budget request remains flat for a third year in a row? How does the administration define “detention reform” and what specific programs, changes, and other activities does the administration are directed to implement detention reform? What specific increases in the ICE budget does the administration count as meeting the planned detention reforms?

Answer. The fiscal year 2012 budget request includes the resources necessary to meet U.S. Immigration and Customs Enforcement’s (ICE) detention and removal goals, including detention reform. In order to make the most efficient use of tax-

payer resources, ICE is seeking efficiencies in detention and removal through targeted efforts that allow ICE to use its resources as efficiently and effectively as possible. These efficiencies include the suspension of detention operations at costly facilities, converting contractors to Federal staff where this will improve service and cut costs, and reducing the average length of stay to allow more detainees to be removed using the same number of beds.

Detention reforms facilitate the detention of individual aliens in settings commensurate with factors such as threat to the community, criminal history, risk of flight, immigration status, stage in the removal process, and medical and mental health. ICE has made substantial progress in a number of critical areas, including access to family and legal visitation, consolidation of facilities, aligning bed space with apprehensions, reducing transfers, improving medical delivery, reducing costs, and developing safe and secure civil detention principles. The following reflect accomplishments and continuing work on detention reform:

- Established an Office of Detention Policy and Planning (ODPP) to plan and design a detention system better tailored to ICE's needs and reforms.
- Consolidated the number of facilities at which ICE detains individuals from 341 to 270 based on state-of-the-art forecasting tools.
- Developed a procurement plan to ensure that future bed space is aligned with apprehensions, thus limiting the need for transfers and ensuring detainees remain closer to their families and attorneys.
- Launched the online detainee locator system, a public, easy to use Internet-based tool designed to assist family members, attorneys and other interested parties in locating detained aliens in ICE custody.
- Hired and trained 42 full-time equivalent detention service managers to monitor conditions at detention facilities, which house 85 percent of the detained population.
- Improved medical services by simplifying the process for the delivery and auditing of authorized healthcare treatments.
- Initiated the creation of a new civil detention facility in Karnes County, Texas, through an intergovernmental service agreement, incorporating new civil detention principles.
- Opened two new facilities in Orange County, California, to reduce the number, costs, and deportation delays associated with detainee transfers.
- Formed two advisory groups of local and national organizations that are stakeholders in the immigration detention system to provide feedback and input to the ICE Director.
- Established an ICE Office of Detention Oversight (ODO) within the Office of Professional Responsibility (OPR). ODO has regional offices to ensure agents and personnel have more ready access to facilities to conduct routine and random inspections more frequently.
- Evaluated and initiated procurements for securing new detention bed space where it is needed most.
- Designed and tested a new detainee intake risk assessment process to provide transparency and uniformity in the detention and classification processes to ensure the prioritization of detention resources.
- Drafted a policy to reduce out-of-region transfers of detainees who have community ties or attorneys of record.
- Drafted revised performance-based national detention standards, in collaboration with members of the Assistant Secretary's Detention Advisory Group, which detail guidelines for the custody and care of ICE detainees.

ICE is committed to instituting detention reform in a fiscally responsible manner that represents the most efficient use of taxpayer resources.

WORKSITE ENFORCEMENT

Question. The administration claims that significant strides have been taken in the past 2 years to increase worksite enforcement efforts. These have focused almost exclusively on the so-called I-9 (employment form) document inspections. While it is important to target and take punitive legal action against unscrupulous employers who knowingly hire illegal aliens, this is largely a paper-based enforcement process. In many cases, the employers claim innocence and fire the undocumented workers. But as one employer commented to the media during the recent investigations of a national fast food company's hiring practices, "The illegal workers just go down the street and get a job at the next food place." In order to ensure that enforcement serves as a deterrent, the administration must also take action against the illegal workers as well as those who seek to knowingly employ them.

Please describe the I-9 process. For the record, please describe the difference between a criminal and administrative arrest in the context of worksite enforcement. How many of each occurred in fiscal years 2006-2010, and how many are estimated to occur in fiscal years 2011 and 2012? How many employers received jail time/sentences as a result of these actions in each of these fiscal years? How many workers were removed or otherwise left the country as a result of these actions in each of these fiscal years (estimates, if necessary). How much in fines was collected as a result of these actions in each of these fiscal years? For fiscal year 2010, the Congress directed ICE to achieve a level of worksite enforcement effort of \$134 million. Is it ICE's intention to meet this goal in fiscal year 2011 as well? Please describe how the agents achieve this level of effort?

Answer. [Follows:]

Form I-9 Inspection Overview

Section 274A(b) of the Immigration and Nationality Act (INA), codified in 8 U.S.C. § 1324a (b), requires employers to verify the identity and employment eligibility of all individuals hired in the United States after November 6, 1986. 8 C.F.R. § 274a.2 designates the Employment Eligibility Verification Form I-9 (Form I-9) as the means of documenting this verification. Employers are required by law to maintain for inspection original Forms I-9 for all current employees. In the case of former employees, retention of Forms I-9 are required for a period of at least 3 years from the date of hire or 1 year after the employee is no longer employed, whichever is longer.

The administrative inspection process is initiated by the service of a Notice of Inspection (NOI) upon an employer resulting in the facilitation of Forms I-9 to ICE officials. ICE typically will allow the employer 3 business days to present the Forms I-9. Often, ICE will request the employer provide supporting documentation, which may include a copy of the payroll, list of current employees, Articles of Incorporation, and business licenses.

ICE agents or auditors then conduct an inspection of the Forms I-9 for compliance. When technical or procedural violations are found, an employer is given 10 business days to make corrections. An employer may receive a monetary fine for all substantive and uncorrected technical violations.

Employers determined to have knowingly hired or continued to employ unauthorized workers will be required to cease the unlawful activity, may be fined, and may be prosecuted criminally. Additionally, an employer found to have knowingly hired or continued to employ unauthorized workers may be subject to debarment by ICE, meaning that the employer will be prevented from participating in future Federal contracts and from receiving other Government benefits. Monetary penalties for knowingly hire and continuing to employ violations range from \$375 to \$16,000 per violation, with repeat offenders receiving penalties at the higher end. Penalties for substantive violations, including the failure to produce a Form I-9, range from \$110 to \$1,100 per violation. In determining penalty amounts, ICE considers five factors: the size of the business, good faith effort to comply, seriousness of violation, whether the violation involved unauthorized workers, and history of previous violations. ICE will notify the audited party, in writing, of the results of the inspection once completed.

In instances where a Notice of Intent to Fine (NIF) is served, charging documents will be provided specifying the violations committed by the employer. The employer has the opportunity to either negotiate a settlement with ICE or request a hearing before the Office of the Chief Administrative Hearing Officer (OCAHO) within 30 days of receipt of the NIF. If the employer takes no action after receiving a NIF, ICE will issue a Final Order. If a hearing is requested, OCAHO assigns the case to an Administrative Law Judge (ALJ), and sends all parties a copy of a Notice of Hearing and Government's complaint, thus setting the adjudicative process in motion.

The Notice of Hearing spells out the procedural requirements for answering the complaint and the potential consequences of failure to file a timely response. Many OCAHO cases never reach the evidentiary hearing stage because the parties either reach a settlement, subject to the approval of the ALJ, or the ALJ reaches a decision on the merits through dispositive prehearing rulings. Employers determined to have knowingly hire or continuing to employ violations shall be required to cease the unlawful activity and may be fined.

Employer Arrests

ICE tracks criminal arrests of employers (inclusive of managers, supervisors, and owners) for worksite enforcement related crimes:

—Fiscal year 2010 = 196 criminally arrested.

- Fiscal year 2009 = 114 criminally arrested.
- Fiscal year 2008 = 135 criminally arrested.
- Fiscal year 2007 = 92 criminally arrested.
- Fiscal year 2006 = 110 criminally arrested.

In fiscal year 2010, ICE's Office of Homeland Security Investigations (HSI) arrested 196 employers for worksite related crimes. As of February 8, 2011:

- 42 were sentenced to prison. Sentences ranged from time served to 42 months.
- Note: 125 cases are still pending a disposition.

DHS defers to the Department of Justice to answer jail time/sentences prior to fiscal year 2010, as criminal sentencing falls under the auspices of the U.S. Attorneys' Offices and ICE did not track sentencing of worksite enforcement violators prior to fiscal year 2010.

Removals

ICE does not track the specific number of illegal aliens removed as a result of being identified during a worksite enforcement operations. Due to the complexity of analyzing the data—hand tabulation and manually crosschecking against several unique law enforcement databases—identifying the removals that resulted from worksite enforcement actions is not available to be included in this response.

Fines Collected

Civil fines resulting from Form I-9 inspections (the final judgment is referred to as a Final Order).

- Fiscal year 2010 = 237 Final Orders \$6,956,026.
- Fiscal year 2009 = 52 Final Orders \$1,033,291.
- Fiscal year 2008 = 18 Final Orders \$675,209.
- Fiscal year 2007 = 2 Final Orders \$26,560.
- Fiscal year 2006 = 0.

Criminal investigations worked in coordination with the Department of Justice, (worksite judicial fines, forfeitures, or restitutions).

- Fiscal year 2010 = \$36,611,320.
- Fiscal year 2009 = \$32,578,945.
- Fiscal year 2008 = \$21,978,917.
- Fiscal year 2007 = \$31,426,443.
- Fiscal year 2006 = \$233,044.

Worksite Enforcement

Since January 2009, ICE has audited more than 4,600 employers suspected of hiring illegal labor, debarred more than 315 companies and individuals, and imposed approximately \$59 million in financial sanctions—more than the total amount of audits and debarments than during the entire previous administration.

ICE expended \$127,436,000 for worksite enforcement related investigations in fiscal year 2010. ICE is projecting for fiscal year 2011 it will expend approximately \$135.2 million. ICE has communicated to the field that worksite enforcement is a high investigative priority for fiscal year 2011.

TRANSPORTATION SECURITY ADMINISTRATION—SCREENER CAP

Question. The House passed a continuing resolution for fiscal year 2011 includes a provision that would limit the number of TSA screeners at 46,000 full-time equivalent screeners. The budget request for fiscal year 2012 includes 48,537 full-time equivalent screeners, not including managers. How would this cap limit TSA's ability to provide security at airports? Explain how advances in technology have allowed screener resources to be used more efficiently. Please quantify how screeners have been reassigned to other security duties as a result of these efficiency gains.

Answer. The continuing resolution for fiscal year 2011 contains a provision limiting the number of full-time equivalents and does not include part-time personnel. Since TSA employs a substantial number of part-time personnel, its fiscal year 2012 budget request for additional Transportation Security Officers (TSOs) to staff advanced imaging technology machines will not be affected. Future growth of full-time personnel may be limited because of the cap, thus restricting TSA's options to reduce attrition and improve the workforce.

Advances in technology most often result in improved effectiveness of the TSOs more so than improved efficiency. One area that TSA has seen improvements in effectiveness and efficiency is the installation of inline baggage screening systems. Inline explosive detection systems are the main technology used in the checked baggage screening process. This equipment automates what was previously a manually intensive baggage inspection, allowing faster bag throughput (up to 300 percent)

and improved threat detection capabilities. These savings have been used to fund other security initiatives and have been considered in the budget request.

The below reflects examples of other security initiatives that efficiency savings have been applied as of fiscal year 2010:

	Total budgeted FTE	Self-funded FTE	Percent of FTE self-funded
Travel Document Checker	2,001	1,086	54
Target Random Security Plays	1,654	904	55
Behavior Detection Officers	2,986	2,326	78
Bomb Appraisal Officers	352	297	84
Total	6,993	4,613	66

AUTOMATED TARGET RECOGNITION

Question. TSA has a delicate balance to maintain when it comes to security and maintaining the privacy of passengers. According to TSA, the Advanced Imaging Technology (AIT) units being deployed to airports across the country are the most effective passenger screening technology currently available because they can detect metallic and nonmetallic threats. However, the images these machines produce of the human body are revealing. TSA is testing a software upgrade to the AIT machines, called Automated Target Recognition, that would do away with the more revealing image and replace it with a generic outline of a person. How is this testing progressing and when do you expect this software to be deployed to airports? TSA's budget request includes funding for 275 additional AIT units in fiscal year 2012 for a total of 1,275. What percentage of passengers will be screened by AIT if the request is funded?

Answer. Automatic Target Recognition (ATR) is currently being tested at Las Vegas McCarran International Airport (LAS), Ronald Reagan National Airport (DCA), and Hartsfield-Jackson Atlanta International Airport (ATL). This testing allows TSA to ensure the new software continues to provide a high level of security, while further enhancing privacy protections. By the end of fiscal year 2012, TSA estimates that 1,275 AITs will be deployed.

BAGGAGE FEES

Question. In recent years, airlines began to charge fees for services that did not previously exist, such as charges for checked baggage. As a result of the new checked baggage fees, more passengers are opting to carry their bags onboard the aircraft causing a strain on security operations at airport checkpoints.

When you testified before the subcommittee, you mentioned that the cost of additional staffing and equipment required to handle the increase in carry-on bags is approximately \$260 million annually. I asked if you thought the airlines should help defray the additional security costs associated with their baggage fees. You responded by saying passenger security fees needed to be adjusted upward. What is your position on whether the airlines should help defray the additional security costs associated with their baggage fees? Without adding more staff and equipment to handle the increase in carry-on bags, will wait times increase because of the baggage fees?

Answer. TSA agrees that increased aviation security costs should not be paid solely by air travelers. When TSA was created, the Congress authorized the establishment of two separate security fees to fund the Federal aviation security costs. One fee was to be paid by air passengers and the other paid by air carriers.

The September 11th Security Fee (Passenger Fee), to be paid by air passengers, was authorized by the Congress to not exceed \$2.50 per enplanement. The revenue generated from this security fee was intended to offset the Federal cost for passenger and property screening. To the extent that revenue derived from the Passenger Fee was not sufficient to cover the Federal cost of passenger and property screening, the Congress authorized the collection of a second security fee to be paid by air carriers.

The Aviation Security Infrastructure Fee (Carrier Fee) was authorized in an amount not to exceed the costs air carriers incurred for passenger and property screening in calendar year 2000. That exact cost total, which TSA originally estimated at \$750 million, has been the subject of much debate and multiple legal proceedings. After an April 2005 Government Accountability Office review of the costs in question, TSA established the overall cap of the Carrier Fee at \$448 million. The

Congress then made this TSA determination subject to judicial review. TSA is still working through the United States Court of Appeals for the District of Columbia Circuit to achieve a final resolution of the overall Air Carrier Fee industry cap that currently stands at \$420 million.

With respect to adjusting the Air Carrier Fee, it is clear that the aviation security enhancements implemented by the TSA since 2001 have made commercial air travel safer for passengers, air carriers and the United States in general. Further, TSA has seen a notable change in carryon baggage volume—increasing checkpoint requirements and processing times—since baggage fees were introduced by air carriers. Under TSA's current staffing model, wait times will likely increase and remain above historical levels that were achieved prior to airline baggage fees. This air carrier action could result in growing passenger wait times and larger concentrations of passengers waiting at checkpoint. To sustain passenger throughput, TSA would need to divert resources from other important security layers or add new personnel to open lanes faster and keep them open longer. TSA has taken some steps to assist in managing wait times. TSA estimates it would cost approximately \$260 million in additional resources to support passenger throughput rates and not detract from other security programs.

DHS FEE PROPOSALS

Question. The President's budget proposes that the Appropriations Committee increase aviation security fees on airline passengers by \$590 million and border inspection fees by \$110 million. Both of these are legislative matters under the jurisdiction of other committees.

Your entire \$459 million proposed increase for TSA and \$55 million of your Customs and Border Protection budget are predicated on our approving these requests.

If the House fails to include these fee increases in their bill, our entire bill would be out of order on the Senate floor if we approved them. The border inspection fee could result in our bill being blue-slipped in the House.

This is a high-risk strategy to support needed security improvements, such as additional Advanced Imaging Technology machines at our airports and improved passenger and cargo inspections on our borders.

What specific steps are you taking to get the House and Senate authorizing committees to request that the House and Senate appropriations subcommittees to approve these legislative proposals?

If the authorizing committees object to our approving these changes in law, will you modify your budget requests to either provide more funding or identify proposed cuts?

Please submit for the record the letters written to the committees of jurisdiction requesting the legislative changes for these requests.

Answer. The President's budget request includes closely related fiscal and policy matters for the Congress's consideration, and the Department looks forward to working with the Congress to provide funding to meet these important security needs.

I fully appreciate the constraints of the current fiscal environment, and it is precisely because of the current economic situation that nothing should be left off the table to fund the Department's critical frontline operations. While airlines have increased fees across the board—from checked baggage and extra leg room to refreshments, we have never adjusted how we fund security measures to protect the traveling public.

Despite the Congress's original intent that the Security Fee covers nearly all costs related to passenger and property screening, the fee currently offsets less than one-third of the total cost of aviation security. At the same time, costs of security have continued to increase. In 2000, it cost less than \$1 to screen each passenger. In fiscal year 2010, the average cost for TSA to screen a passenger and baggage has increased to nearly \$9, in part to airline imposed checked baggage fees that have resulted in TSA screening 56 million additional carry-on bags at airport checkpoints annually.

As such, I have personally discussed with members of congressional authorizing committees the request to permit DHS to increase the Security Fee, and the Department will continue this outreach. The Department will also continue to engage members of the authorizing committees on all legislative provisions necessary to support the budget request to ensure passage of stand alone legislation or to help secure support for provisions which may be carried in appropriations measures, whichever occurs first.

With regard to the proposed CBP fee change, the country exemptions currently in place for Mexico, Canada, and the Caribbean cost the Government \$110 million

annually in user fees that would otherwise be collected for customs inspections at the border. While travelers from other countries are subject to this fee, the costs of processing the travelers coming from Mexico, Canada, and the Caribbean are subsidized by United States taxpayers. CBP's budget assumes elimination of these exemptions by the third quarter of fiscal year 2012, equating to \$55 million in fiscal year 2012 (half-year cost).

AVIATION SECURITY CAPITAL FUND

Question. The request includes a legislative proposal to alter the manner in which offsetting collections from the Aviation Security Capital Fund are allocated. Has the Department made a request to the subcommittee with jurisdiction over this matter? If so, please submit the request for the record. The language states that the funds "may be distributed in any manner deemed necessary to ensure aviation security." Would any of these funds be used for purposes other than checked baggage security? Please be more specific on how the funds would be distributed to support aviation security in fiscal year 2012. What is the impact of not receiving this language adjustment in fiscal year 2012?

Answer. The Department's request for this legislative proposal to provide the Department with the required flexibility to sustain current security measures and adapt to emerging threats was transmitted to each committee with oversight of DHS along with the fiscal year 2012 President's budget request. Due to the importance of this proposal, I have had discussions with members of the authorizing committees and representatives of the Department's Office of the Chief Financial Officer have briefed committee staff on the request to permit the Department to increase the Security Fee. We will continue to engage members of the authorizing committees on all legislative provisions necessary to support the budget request as long as necessary to ensure passage of stand alone legislation or to help secure support for provisions which may be carried in appropriations measures, whichever occurs first.

The current law requires that the first \$250 million derived from passenger and air carrier security fees in each of the fiscal years 2004 through 2028 be deposited in an Aviation Security Capital Fund (ASCF) to be available for grants to airport sponsors for airport security improvement projects such as facility modifications. The language currently does not allow for the procurement and installation of EDS equipment for the security improvement projects. The legislative proposal included in the fiscal year 2012 budget request would permit approximately \$125 million of the ASCF to support the recapitalization and deployment of state-of-the-art EDS for checked baggage to efficiently screen baggage for explosives, reducing the number of rescans and physical bag searches. The remaining \$125 million would be used for airport facility modification projects. The current notional plan is summarized in the following table:

BREAKDOWN OF PLANNED ACSF OBLIGATIONS ¹

[Dollars in millions]

Projects/equipment	Amount
Medium Speed EDS Purchase	94
Medium Speed EDS Installation	31
Facility Modifications	125
Total	250

¹ Numbers based on notional plans as of 2/9/11 and are subject to change.

By 2013, nearly one-half of the 2,000 EDS units deployed nationwide will have exceeded their planned 10-year service life. Limiting TSA's ability to purchase and install equipment as needed could increase the risk of equipment failure and lead to increased delays at airports due to the need to rescan baggage and conduct physical bag searches.

EXPLOSIVES DETECTION SYSTEMS

Question. The request states that of the 2,000 explosives detection system units currently deployed nationwide, almost one-half will have reached the end of their useful life of 10 years by 2013. How much of the \$273 million discretionary request for explosives detection systems would be used for this purpose in fiscal year 2012. How many machines would be replaced? If the legislative proposal to adjust the manner in which offsetting collections from the Aviation Security Capital Fund are

allocated is approved, how much of the \$250 million would be used for this purpose in fiscal year 2012. How many machines would be replaced?

Answer. Of the \$273 million in discretionary funding requested in fiscal year 2012, TSA would use \$14 million to replace 26 reduced size explosives detection system (EDS) units that have reached the end of their useful life. With approval of the Aviation Security Capital Fund (ASCF) legislative proposal, TSA would use \$125 million of the \$250 million fund to replace the 63 medium speed EDS units that have reached the end of their useful life.

The remaining \$259 million of the EDS discretionary funds would be used for the following manner:

- \$130 million for the purchase and installation equipment for facility modifications that have already been executed or plan to be executed in fiscal year 2012.
- \$129 million for technology and engineering (T&E) initiatives and program operations and management (PO&M) support, which includes \$40 million for testing and engineering support; \$24 million for program support to include warehouse leasing and TSIF operations; \$18 million to support cargo and surface; and \$19 million for Federal personnel compensation and benefits.

If the legislative proposal is not adopted TSA's recapitalization of equipment would be delayed.

Question. The budget request indicates that 55 of the top 85 airports had optimal checked baggage screening systems throughout the entire airport and another 22 have optimal screening systems in some part of the airport. With the \$523 million in discretionary and mandatory funds requested in 2012, how will these figures change? When does TSA estimate having optimal systems at all 85 airports? What are the main drivers preventing completion of systems at the remaining airports?

Answer. Given that more than two-thirds of the explosives detection systems (EDS) in the field will reach the end of their useful life in the next 5 years, TSA has shifted its priorities from completing optimal systems to the recapitalization of the aging EDS fleet. The \$523 million in fiscal year 2012 funding and prior year carryover funds will primarily be used to accommodate airport growth, recapitalization and/or optimization of existing equipment at multiple airports. Optimal systems are expected to be completed at two additional category X and I airports with fiscal year 2012 and prior year funds.

BEHAVIOR DETECTION OFFICERS

Question. The request includes funding for an additional 350 Behavior Detection Officers (BDOs). The Government Accountability Office (GAO) released a critical report on this program in 2010. Please explain the steps TSA has taken to address the concerns raised by GAO.

Answer. TSA's BDOs are an important layer of aviation security. Screening Passengers by Observation Techniques (SPOT) builds on and is based on other established, successful behavioral analysis programs that have been employed by law enforcement and security personnel both in the United States and around the world. The Department of Homeland Security's (DHS) Science and Technology Directorate (S&T) led a comprehensive study to validate the validity of TSA's SPOT Referral Report. Data collection was completed by TSA in late 2010 and provided to the American Institutes for Research for analysis and reporting. The validation study report is undergoing final review and S&T testified before the House Science, Space, and Technology Committee, Subcommittee on Investigations and Oversight on this topic on April 6. Preliminary briefings on the validation study data indicated that SPOT identifies high-risk travelers at a significantly higher rate than random selection.

Additionally, TSA's risk analysis of SPOT indicates that the program can be effective in multiple threat scenarios and expanding the SPOT program increases TSA's ability to adapt to evolving threats. S&T completed a preliminary study on suicide bomber indicators in July 2009 that illustrates overlap between some operationally reported suicide bomber indicators and certain TSA SPOT behaviors. As such, SPOT represents the best practices from defense, intelligence, and law enforcement organizations.

TSA also began piloting SPOT refresher training for BDOs in March 2011 and plans to deploy this training to all BDOs during fiscal year 2011 and fiscal year 2012.

SCREENING PROCEDURES

Question. The Administrator has said publicly that he intends to introduce new screening measures this year that would be different than the "one size fits all" approach. Does the fiscal year 2012 budget request account for these changes? Please

explain in more detail how this new screening process will work and the schedule to implement it.

Answer. TSA will introduce new risk-based screening procedures and enhance current technology for passenger screening as it continually evolves its layered approach to transportation security. TSA is exploring the possibility of piloting these concepts later this year. The fiscal year 2012 budget request will not require adjustment to incorporate additional risk-based screening principles.

CHECKPOINT SECURITY

Question. TSA is in the process of updated its checkpoint security strategic plan. What is the timeline for its completion?

Answer. TSA anticipates completing the updated Passenger Screening Program Strategic Plan by summer 2011.

CIVIL RIGHTS AND CIVIL LIBERTIES

Question. What is the funding level and associated staffing for TSA's Office for Civil Rights and Civil Liberties? Describe TSA's coordination with the Department's Office for Civil Rights and Civil Liberties? How many civil rights and civil liberties investigations did TSA conduct in 2010? How many of those investigations were conducted jointly with the Department Office for Civil Rights and Civil Liberties? What training standards must a TSO meet with regard to civil rights and civil liberties?

Answer. The fiscal year 2011 budget includes \$8.7 million total funding for TSA's Office of Civil Rights and Civil Liberties (OCRL) which demonstrates our commitment to ensuring the traveling public's civil rights and civil liberties are protected throughout the screening process. The TSA OCRL coordinates closely with DHS CRCL to address concerns and complaints of the traveling public through meetings with community groups, employee training, policy reviews, and investigations into traveler complaints. In fiscal year 2010, TSA conducted 217 internal investigations and 42 external investigations. There were no investigations conducted jointly in fiscal year 2010 by the Department and TSA. To date in fiscal year 2011, there are four joint investigations open. TSOs must complete training annually focusing on cultural awareness, civil rights and civil liberties. Additionally, No FEAR Act Training must be completed within 90 days of entering service. This training is required pursuant to the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 and provides an overview of Federal antidiscrimination and whistleblower protection laws. This training regimen is repeated every 2 years.

TSA INTERNAL AFFAIRS

Question. How many people are in TSA's internal affairs office? Is TSA adding new positions in fiscal year 2011? Are any new positions requested in the President's budget for fiscal year 2012? Is TSA creating an Office of Professional Responsibility? What role will this office serve? How is TSA funding this effort and how many people will staff the office?

Answer. TSA currently has 130 personnel that conduct internal investigations in the Office of Inspection (OOI). Under the proposed fiscal year 2011 continuing resolution, no new positions will be funded and there are no new positions requested for the OOI in the fiscal year 2012 President's budget.

TSA established the Office of Professional Responsibility (OPR) in the fall of 2010 to provide greater consistency in misconduct penalty determinations and a more expeditious and standardized adjudication process. Through a combination of adjudication and oversight, OPR ensures that discipline is appropriate and fair for all TSA employees, regardless of the assignment or seniority of the employee involved.

In addition, to promote consistency, TSA is transferring to OPR from the Disciplinary Review Board (DRB) the responsibility for resolving TSO's appeals of adverse actions, including suspensions of 15 days or greater, removal, or reduction in pay band or basic rate of pay. This will preserve the rights of TSOs to appeal actions taken by management while enabling OPR to ensure that discipline is consistent across the board, from senior-level officials to TSOs.

TSA is funding OPR from within existing sources. OPR has 15 positions that are being filled through a combination of vacancy announcements and internal detail opportunities. OPR is also absorbing four positions from the Disciplinary Review Board, for a total of 19 OPR positions.

SURFACE TRANSPORTATION

Question. How much of TSA's surface transportation appropriation is dedicated to each surface transportation mode for fiscal year 2011 compared to the fiscal year 2012 estimate?

Answer. Under the funding that is currently available, the TSA surface transportation appropriation is dedicated to each surface mode in the following ways: 28 percent to Surface Inspectors and Program Oversight; 25 percent to Visible Intermodal Prevention and Response Teams; 13 percent to Freight Rail and Pipeline; 12 percent to Ports (Maritime) and Intermodal Security; 11 percent to Highway and Motor Carrier; 8 percent to Mass Transit; and 3 percent to other services. The fiscal year 2012 President's budget request includes \$134.7 million to support TSA's surface transportation efforts and also includes \$300 million for the Transit Security Grant Program (TSGP) to support State and local surface transportation efforts. TSA will allocate the funding to each surface transportation mode based on current security efforts to reduce risk once the funds have been appropriated.

Question. How much of TSA's budget in fiscal year 2010 and fiscal year 2011 was dedicated to mass transit enhanced screening? Where the pilots successful? Does TSA have plans to continue the pilots? Does the fiscal year 2012 budget include funding for this purpose?

Answer. In fiscal year 2010, the Congress provided TSA \$25 million for partial year funding to stand-up an additional 15 visible intermodal prevention and response (VIPR) teams for dedicated surface transportation operations. This was in addition to TSA's 10 multimodal VIPR teams already operational. During fiscal year 2010, approximately 51 percent of TSA's VIPR resources were spent conducting operations in the surface modes of transportation, which equates to approximately \$22 million. The primary objective of VIPR operations is to prevent acts of terrorism through the exercise of random, unpredictable security asset deployments in all modes of transportation and this may include mass transit enhanced screening.

In fiscal year 2010, TSA entered into an agreement with New York City to conduct pilot or proof of concept operations with New York City law enforcement for mass transit screening. This effort involved approximately 35 TSA TSOs teamed with New York City law enforcement officers operating in shifts with approximately 3 TSOs. This proof of concept was successful in terms of demonstrating the ability to work together in teams and build expertise in the environment to allow for improved security in response to specific threats requiring surge operations or in response operations. TSA has no plans to continue or expand this proof of concept.

Such efforts will continue to be supported by other TSA surface transportation initiatives, including the additional VIPR teams and funding available through the TSGP, which supports local efforts to conduct enhanced screening. Such physical screening can be conducted as necessary by applicable State, local, or private personnel with equipment available through the TSGP (e.g., explosives trace detection equipment).

The fiscal year 2012 budget request seeks funding for 12 new multi-modal VIPR teams. With these additional teams, the VIPR program anticipates an increase in tempo for a total number of 11,500 operations to be conducted annually beginning with fiscal year 2013. These operations would be conducted throughout the transportation sector to deter potential terrorist acts.

FEDERAL AIR MARSHALS

Question. Please provide the most recent definitions of high-risk flight categories for flights covered by Federal Air Marshals (FAMs). Are these definitions being revised, and if so, how will the changes impact the deployment of FAMs.

On March 8, 2011, the Department submitted a report on Federal Air Marshals (FAMS) long-term staffing levels in response to a fiscal year 2010 congressional requirement in the joint explanatory statement accompanying the fiscal year 2010 DHS Appropriations Act. The report failed to address the congressional requirements for a long-term staffing plan and pointed to an assessment TSA will undertake to review FAMS risk-level definitions in order to inform an assessment of the long-term staffing needs of the FAMS. When will this assessment be completed? The results of this assessment and associated staffing impacts are to be supplied to the subcommittee expeditiously.

Answer. The TSA has commenced a review of FAMS risk-level definitions, which will be provided to the subcommittee upon its completion. The review will inform any decisions pertaining to the long-term staffing levels needed in the future.

COAST GUARD—ADMINISTRATIVE SAVINGS

Question. The fiscal year 2012 request for the Coast Guard's operating budget includes a reduction of \$83.5 million as part of the Department's Administrative Savings Initiative. When you read the fine print, the Coast Guard's budget states that these cuts "do not come without impact to readiness and operations." The Coast Guard is already facing readiness challenges and operational shortfalls. How are these cuts prudent? Can you provide more specifics on how these cuts will impact readiness and operations?

Answer. The Coast Guard's fiscal year 2012 budget leverages savings generated through management efficiencies and offsets to prioritize front-line operations and investments in vital recapitalization projects. The Coast Guard will not reduce front-line operations to achieve these savings. The fiscal year 2012 budget request addresses the long-term recapitalization needs of the Coast Guard and expands its operational capacity by funding 50,682 military and civilian positions, including additional personnel focused on strengthening Marine Safety inspections and investigations as well as a new Incident Management Assistance Team, which will be deployed rapidly to support large-scale emergencies.

IMPACT OF 2010 COAST GUARD SURGE OPERATIONS

Question. In 2010, the Coast Guard's operational budget was stretched with two significant surge operations, the Haiti earthquake and Deepwater Horizon Oil Spill. Given the size of these surge operations, what was the impact on spending for other priorities? What was deferred or eliminated to pay for these response efforts?

Answer. The Coast Guard allocates its multi-mission assets to the Nation's highest order needs. In the cases of the operational responses to the Haiti earthquake and Deepwater Horizon Oil Spill, assets were diverted from other lower priority mission assignments at the time to provide the initial search and rescue response and long-term mission support for the disasters.

The Supplemental Appropriations Act, 2010 (Public Law 111-212) provided \$50 million in operating expenses for the Coast Guard related to expenses for disaster response activities for the Haiti earthquake. The funding provided relief to the Coast Guard for operating and personnel costs expended for the response.

For the BP Deepwater Horizon Oil Spill, the Coast Guard's direct costs, including supplies purchased for the spill, contractors hired, travel orders, and reservist pay and benefits were reimbursed from the Oil Spill Liability Trust Fund (OSLTF) Emergency Fund and the Fund recovered those costs from the Responsible Party. Consistent with Coast Guard's multi-mission responsibilities, costs to operate assets diverted from regular operations to the oil spill response were funded by regular appropriations. Due to the unusually long engagement period for response, regular maintenance for some assets was deferred, which could result in higher maintenance costs.

COAST GUARD ASSET DECOMMISSIONINGS

Question. Provide a chart of all assets proposed to be decommissioned in the fiscal year 2012 budget, including the name and location of each asset and timeline for decommissioning.

Answer. The chart below depicts U.S. Coast Guard assets proposed for decommissioning in fiscal year 2012 President's budget.

Asset type	Vessel name	Homeport	Decommissioning date
179-ft Patrol Coastal (WPC) ¹	USCGC <i>Shamal</i> USCGC <i>Tornado</i> USCGC <i>Zephyr</i>	Pascagoula, Mississippi.	WPCs will be returned to the United States Navy no later than October 1, 2011.
378-ft high endurance cutter (WHEC) ² .	To be determined	To be determined	To be determined.

¹ Three vessels are being decommissioned per a signed Memorandum of Agreement with the U.S. Navy in January 2007.

² The Coast Guard is conducting an updated engineering assessment on the 10 remaining WHECs (2 decommissioned in fiscal year 2011) to determine which WHEC will be decommissioned in fiscal year 2012. Factors being considered include operational capabilities and effectiveness of the current fleet and existing structural and engineering conditions of the ships.

POLAR ICEBREAKERS

Question. The budget request includes \$39 million for operations and maintenance of the Coast Guard's polar icebreaking fleet. The Commandant of the Coast Guard has expressed concern that he doesn't have the resources to respond to a major emergency in the Arctic. He has publicly stated that funding is needed to repair or replace its two heavy icebreakers that are currently out of service. But the Coast

Guard's budget indicates that one of the Coast Guard's two heavy polar icebreakers, the *Polar Sea*, will be decommissioned in fiscal year 2011. The other heavy polar icebreaker, the *Polar Star*, is not scheduled to be reactivated until 2013. Why is the Department planning to decommission the *Polar Sea* when long-term requirements for the polar regions have not been determined? If an emergency occurs in the Arctic, is the Coast Guard prepared to respond? What other response capabilities exist? Has the Coast Guard considered leasing polar icebreakers to meet mission requirements?

Answer. Based on current Federal requirements, maintaining and operating one icebreaker (CGC *Healy*) will allow the Coast Guard to meet current operational requirements in the Arctic. Based on the rising costs to maintain the polar icebreakers, which have exceeded their life expectancy, the current condition of CGC *Polar Sea* and her limited remaining service life, leveraging resources to reactivate CGC *Polar Star* as a backup is the proper course of action until long-term requirements decisions are made and capabilities are acquired. The fiscal year 2012 budget includes \$5 million for an analysis of Government-wide icebreaking requirements in the polar regions.

DEPLOYABLE SECURITY TEAMS

Question. Section 804 of the fiscal year 2010 Coast Guard Authorization Act requires no less than two enhanced deployable security teams. The Coast Guard currently has one Maritime Security Response Team located in Portsmouth, Virginia. What are the Coast Guard's plans to comply with section 804? Has a second location been determined?

Answer. Coast Guard has not determined a location for a second enhanced team.

CANINE TEAMS

Question. What is the Coast Guard doing to comply with section 805 of the 2010 Coast Guard Authorization Act regarding canine teams? How many certified canine teams does the Coast Guard currently have and where are they located? Does the Coast Guard have plans to increase capacity in fiscal year 2012? If so, what locations will receive additional canine teams?

Answer. There are currently 12 canine teams certified for duty in the Coast Guard. The Coast Guard has programmed for 14 canine teams that are located in pairs at 7 locations:

- MSST Seattle, Washington.
- MSST San Francisco, California.
- MSST Los Angeles, California.
- MSST Galveston, Texas.
- MSST King's Bay, Georgia.
- MSRT Chesapeake, Virginia.
- MSST New York, New York.

MSST's San Francisco and King's Bay currently have one of their two teams certified. Expected completion of training and certification for the remaining two teams is early calendar year 2012. The Coast Guard does not have plans to increase canine capacity beyond these levels in fiscal year 2012.

MARINE ENVIRONMENTAL PROTECTION

Question. Please provide more details on the Coast Guard's investment in the National Center of Expertise. How much of the \$11.5 million increase for Marine Environmental Protection is dedicated for this purpose? How is the funding for the National Center of Expertise allocated in the request, to what organization, and where?

Answer. The fiscal year 2012 budget request includes funding to establish the National Incident Management Assist Team (IMAT). Although the National IMAT could be a core component of a future MER National Center of Expertise (NCOE), as a stand-alone unit, the National IMAT will also significantly enhance the Coast Guard's ability to respond to complex, large-scale events in the maritime domain. Specifically, the IMAT investment provides dedicated, trained, and experienced personnel to directly respond to oil and hazardous substance spill incidents, and to support Coast Guard Federal On Scene Coordinators during such incidents. They will also provide planning, training, and exercise support across the Coast Guard. Through establishment of the IMAT, the Coast Guard will improve standardization and proficiency in MER across the Coast Guard and its partners.

The fiscal year 2012 cost of the IMAT enhancement is approximately \$5.5 million. Of that, approximately \$3 million will be budgeted to cover personnel expenses associated with 33 full-time positions, and \$2.5 million will be budgeted for operations and maintenance.

PORT SECURITY TRAINING

Question. Describe the process for complying with section 821 of the Coast Guard Authorization Act regarding port security training and certification.

Answer. The Coast Guard plans to implement the training provisions discussed in section 821 via the rulemaking process, pending the Department of Homeland Security's review and approval to the Updates to Title 33 Code of Federal Regulations Subchapter H—Maritime Security Notice of Proposed Rulemaking (NPRM). The NPRM is scheduled for publication in calendar year 2011. Once published, the Final Rule, along with clarifying guidance from the Coast Guard, will be the basis for third party providers' course development and Quality Standards System review and acceptance on behalf of the Coast Guard.

COAST GUARD ACQUISITIONS

Question. The budget request includes a significant increase for shore facilities improvements when compared to previous requests. The Coast Guard estimates that the current backlog of shore facility infrastructure improvements is \$600 million. Is the entire request associated with this backlog?

Answer. \$94.5 million of this request is to support shore facility infrastructure modifications and construction associated with the delivery of new cutters, boats, and aircraft. The remaining \$99,200,000 of the \$193.7 million request for shore facilities, plus the \$20 million requested for military family housing, help address the backlog in the prioritized Shore Facility Requirements List.

Question. The budget proposes to eliminate the Integrated Deepwater Construct. Is there a plan for tracking the Coast Guard's ongoing acquisition costs in relation to the original Deepwater baseline? If so, what assets will be included in the baseline?

Answer. The fiscal year 2012 President's budget proposes the elimination and disaggregation of the Integrated Deepwater System (IDS) subappropriation from the Coast Guard's Acquisition, Construction and Improvement (AC&I) appropriation. The restructuring of this appropriation better enables the service to justify and meet a sustainable, stable, and continuous recapitalization program while effectively managing cost, schedule, and performance of individual asset-based acquisitions. Enacting this proposal will further enhance acquisition management and accountability by aligning the appropriations structure with how the projects are managed. This initiative improves transparency and accountability by establishing a stronger linkage between appropriations and specific asset acquisition projects, and will better enable the Coast Guard, DHS headquarters, and the Congress to monitor cost, schedule and performance of individual projects. Finally, disaggregation of the IDS subappropriation will improve the efficiency and effectiveness of cross-cutting functions, such as systems integration, testing, and performance monitoring, enabling uniformity across all acquisition projects. The Coast Guard will retain its ability to track to the Deepwater baseline in aggregate.

Question. What is the rationale for changing funding availability for all Acquisition, Construction and Improvements appropriations to 5 years?

Answer. The Integrated Deepwater System (IDS) appropriation (which included "deepwater" vessels, aircraft and other equipment), was available for 5 years. The proposal to disaggregate the IDS subappropriation in fiscal year 2012 is intended to standardize funds availability for each of the individual vessel, aircraft, other and shore subappropriations, which will ensure consistency in funds availability across the entire portfolio of projects, and enhance the Coast Guard's ability to maintain project cost, schedule and performance goals.

Specifically, the Coast Guard has increased its use of fixed-price contracts for major acquisitions, moving away from cost-reimbursement contracts. This change in strategy decreases overall risk to the Government, but requires the Coast Guard to set-aside funds for antecedent liability (a requirement that does not exist for cost-reimbursement contracts). The Government Accountability Office's Redbook cites that fixed-price contract antecedent liabilities shall be funded by the appropriation that funded the original transaction, to cover within-scope changes associated with the original contract. The amount of unobligated funding (set aside for antecedent liability) can be adjusted and reallocated over time as the contract nears completion, provided that the funds are used within the scope of the project and Congressional intent. The net effect is to avoid the need for additional future appropriations by minimizing expired, unused funds. Moreover, given the complexity of many of the Coast Guard's vessel, shore, aircraft and electronics systems acquisitions, 5-year availability is particularly beneficial considering the time it takes to design, contract, and deliver these assets.

Question. Has the Coast Guard spent any of the \$45 million anticipated for the offshore patrol cutter (OPC) in fiscal year 2011? Is it premature to fund another \$25 million in fiscal year 2012 if none of the fiscal year 2011 money has been obligated? Is the Coast Guard on track to release the request for proposal for the preliminary contract and design in fiscal year 2011?

Answer. The offshore patrol cutter (OPC) is a critical aspect of the Coast Guard's long-term recapitalization plan. Of the funding made available to the OPC project to date under the current series of continuing resolutions, \$1 million has been obligated. The majority of the fiscal year 2011 funding, approximately \$36 million, will support preliminary and contract designs; the remaining funding will support project management activities, acquisition studies and life-cycle cost analysis still planned in fiscal year 2011. The fiscal year 2012 budget request of \$25 million will support the award of Preliminary and Contract Design contracts to three industry teams in fiscal year 2012. The Coast Guard plans to release a draft Request for Proposal in fiscal year 2011.

Question. Will DHS' requirement for the Coast Guard to conduct a verification study of the OPC requirements affect the timeframe for the request for proposal?

Answer. No, the project has proceeded in parallel with the verification study of OPC requirements.

Question. Based on the fiscal year 2012 Capital Improvement Plan (CIP), the cost of the OPC is \$640 million in fiscal year 2015 and \$760 million in fiscal year 2016. Provide a breakdown of the OPC costs in those budget estimates? Why is the second OPC planned to cost \$120 million more than the lead ship?

Answer. The program amounts shown in the fiscal year 2012–2016 Capital Investment Plan for the OPC are planning estimates. These planning estimates may change as DHS completes the fiscal year HSP.

Question. In the fiscal year 2011 CIP, the Coast Guard estimated the national security cutter's (NSC) completion date as 2016. In this year's CIP, the Coast Guard is estimating a completion date of 2018. What are the main drivers behind this 2-year delay? To what extent is the decision to not request long lead time materials for NSC #6 in fiscal year 2012 contributing to this delay? Would there be cost savings if long lead time materials were funded in fiscal year 2012? If so, provide the estimated savings.

Answer. The project completion dates shown in the fiscal year 2012–2016 CIP are estimated for planning purposes, based on best available data at the time of budget preparation. The NSC schedule is derived from the Deepwater Implementation Plan Review Report to Congress, dated May 13, 2010, which contains a more recent assessment of NSC delivery schedules, considering actual appropriations and acquisition status to the date of the report. One factor in the delay in the NSC acquisition was the transition from a cost-plus contract to a fixed-price construct. The Coast Guard spent nearly a year negotiating the production contract for NSC #4, which was awarded in November 2010. As a result of this negotiation and successful transition to a fixed-price construct, the Coast Guard believes it is now in a position in which future costs are more predictable than they have ever been, which is in the best interests of the program and of taxpayers.

The funding associated with NSC #6 is not required until fiscal year 2013.

Question. At the hearing, you made reference to a letter from the Office of Management and Budget that committed funding for NSC #6. Please provide the letter for the record.

Answer. In accordance with the requirements of Public Law 111–83, the Coast Guard submits a future-years capital investment plan at the time that the President's budget is submitted. This plan, the fiscal year 2012–2016 Capital Investment Plan (CIP), was included in the fiscal year 2012 Coast Guard Congressional Justification within the Acquisition, Construction and Improvements (AC&I) appropriation request. The CIP projects planned AC&I funding levels from fiscal year 2012 through fiscal year 2016 for the program of record for each AC&I program, including the NSC program. These estimates are in accordance with the latest Department of Homeland Security-approved Acquisition Program Baseline. As noted in the CIP footnotes, fiscal year 2013–2016 funding levels are subject to change based upon adjustment to out-year fiscal guidance and finalization of the fiscal year 2012–2016 Future Year Homeland Security Program.

Question. Based on the fiscal year 2012–2016 CIP, the Coast Guard is planning the budget for NSC to be \$775 million in fiscal year 2013, \$795 million in fiscal year 2014, and \$853 million in fiscal year 2015. Provide a breakdown of the NSC costs in those budget estimates? Why are NSC costs becoming more expensive for each cutter in the outyears?

Answer. The program amounts shown in the fiscal year 2012–2016 Capital Investment Plan are planning estimates and subject to change as DHS completes the fis-

cal year HSP. The following table shows the estimated costs used as the basis for NSC projections:

[Dollars in millions]

NSC Cost Categories	Fiscal year 2013	Fiscal year 2014	Fiscal year 2015	
	NSC #6	NSC #7	NSC #8	NSC #1/#2
Long Lead Time Materials (LLTM)	114	119	124
Production Contract	578	587	598
Production (Noncontract) and Post Delivery Activities	83	89	93
Structural Enhancement (NSC #1 and #2 only)	38
Total	775	795	815	38

Assuming the new fixed-price construct, the budget estimates for NSCs #6–8 are estimated as the production cost for NSC #4 adjusted for inflation. NSC #7 and #8 costs are projected to continue to increase due to labor and material inflation and increases in projected overhead rates.

Question. The budget proposes to fund production of both the NSC and OPC in fiscal year 2015. Is this a realistic request given the current fiscal environment?

Answer. The Department of Homeland Security is committed to recapitalizing the Coast Guard's cutter fleet as quickly as possible through the acquisition of NSC and OPC and fast response cutters (FRC).

Question. The original plan for the NSC included ship-based UAS to expand the NSC's coverage capabilities. The Coast Guard's Capital Investment Plan for fiscal years 2012–2016 includes no UAS funding. Has the Coast Guard abandoned this effort? What over the horizon search capabilities does the NSC provide over that of a WHEC without UAS? The Coast Guard expected to complete the UAS "Need Phase" (Acquisition Decision Event-1) in fiscal year 2011. What is the status of this effort and, if completed, what were the conclusions from this event?

Answer. The Department of Homeland Security and the Coast Guard remain committed to employing both land and cutter-based UAS to meet mission requirements. The Coast Guard is in the preacquisition Need Phase of the UAS acquisition, which works to define the problem through a mission needs statement and the development of a Concept of Operations. In addition, the Coast Guard is currently leveraging prior-year Research and Development Test and Evaluation funding to continue UAS technology demonstration. Further, within the Federal Government, the Coast Guard has established formal partnerships with Customs and Border Protection to collaborate with their maritime Predator UAS (Guardian) program and the Navy's UAS program offices to collaborate on the Fire Scout program.

An NSC without a UAS, relying solely on its organic detection equipment and manned aircraft patrols, has a far greater surveillance area than that of a high endurance cutter (WHEC). The NSC has the following organic surveillance capabilities that exceed those of the WHEC:

- Ability to operate with a HH-60 enabling greater cutter-based surveillance range and on scene time.
- Ability to deploy and operate with two HH-65 aircraft instead of one from a WHEC.
- Two over-the-horizon (OTH) small boats instead of one from a WHEC.
- Three-dimensional capable air search radar instead of WHEC's two dimensional air search radar.
- Sensitive Compartmentalized Intelligence Facility (SCIF) to improve sensor and intelligence analysis and fusion.
- Enhanced Electronics Surveillance Measures (ESM).

Question. Compare the availability of the national security cutters (*Bertholf*/*Waesche*) to the 12 WHECs in terms of days away from homeport (DAHP).

Answer. The operational target for the WHEC fleet is 185 DAFHP annually per cutter. In fiscal year 2010, the WHEC fleet achieved 137 days away from homeport (DAFHP) primarily as a result of casualties to hull and mechanical systems.

There is not yet substantive DAFHP data for CGC *Bertholf* and CGC *Waesche*. In fiscal year 2010, both assets spent time in planned inport availabilities for Secure Compartmentalized Intelligence Facility installations and Ready for Operations preparations. The Coast Guard will have operational availability data for CGC *Bertholf* after it completes its first full year of operations in fiscal year 2011 for which it is programmed to achieve 185 DAFHP.

Question. In fiscal year 2010, because of delays in the planned delivery of national security cutters, the Congress provided \$4 million for the Coast Guard to conduct a preacquisition survey and design to determine the requirements for a maintenance effectiveness project for the Coast Guard's legacy high endurance cutters. What is the status of this effort and has any of the \$4 million been obligated? What is the timeline for completing this effort?

Answer. A total of \$468,819 has been obligated through March 10, 2011. This funding will be used to adequately assess current WHEC material condition, assess requirements of a potential future sustainment project and inform decisions pertaining to the WHEC decommissioning sequence, and evaluate cutter safety conditions. The Coast Guard anticipates it will take approximately 2 years to complete this effort.

Question. The fiscal year 2012 budget includes \$129.5 million for two Maritime Patrol Aircraft (MPA) airframes and five mission system pallets and spares. Does the Coast Guard plan to buy these pallets through the ICGS contract, use another contracting source, or build them in-house? What is the cost difference for each option?

Answer. The Coast Guard contract with Integrated Coast Guard Systems expired in January 2011 and no additional Mission System Pallets (MSPs) will be procured using that contract vehicle. The Coast Guard does not currently possess sufficient in-house processes and capabilities to be able to produce MSPs "in-house" by 2012. Therefore, acquiring MSPs through a commercial source is the preferred option.

Question. The fiscal year 2012 CIP indicates a 5-year delay in completing procurement of the MPAs when compared to the fiscal year 2011 CIP. What is the cause of this delay?

Answer. The project completion dates for the Marine Patrol Aircraft (MPA) shown in the fiscal year 2012–2016 CIP are estimated for planning purposes, based on best available data at the time of budget preparation. The MPA schedule is derived from the Deepwater Implementation Plan Review Report to Congress, dated May 13, 2010, which contains a more recent assessment of MPA delivery schedules.

Question. The request includes funding for five MPA mission pallets. What is the cost savings from purchasing multiple mission pallets in fiscal year 2012?

Answer. Ordering five MSPs instead of two is estimated to reduce the MSP unit price by as much as 30–35 percent based upon previous negotiations.

Question. Does purchasing six FRCs in fiscal year 2012 maximize the contract? What is the cost savings by maximizing the contract in fiscal year 2012?

Answer. Yes, procuring six FRCs in fiscal year 2012 maximizes the contract. The average cost savings per hull is approximately \$5 million including production costs, economic price adjustments associated with spare parts, antecedent liabilities and other scalable program costs (e.g., project management, testing, certification, etc.).

UNITED STATES SECRET SERVICE—PRESIDENTIAL CAMPAIGNS

Question. Provide the number of candidates and number of protection days for Presidential campaigns going back to 1996, including costs.

Answer. [Follows:]

Campaign (fiscal year)	Protection days	Candidates/ nominees	Spouses/adult children	Cost ¹
2008	1,115	5	6	\$70,304,000
2004	454	3	2	38,686,000
2000	452	4	3	27,787,000
1996	364	4	2	16,459,000

¹Presidential campaign costs do not reflect the "labor shift" of existing base resources from investigative programs to support the protection demands of the campaign.

ASIA-PACIFIC ECONOMIC COOPERATION SUMMIT COSTS

Question. Provide detail on how much funding is needed in fiscal year 2011 for the Asia-Pacific Economic Cooperation (APEC) Summit in Honolulu, Hawaii.

Answer. Total estimated cost that the U.S. Secret Service will incur in fiscal year 2011 for the Asia-Pacific Economic Cooperation (APEC) Summit is \$5.4 million. These cost include airfare, vehicle rental, housing, and per diem cost of personnel who have been temporarily reassigned (TDY) to Honolulu, Hawaii since October 2010 to prepare for this National Special Security Event (NSSE). Additionally, these costs include the rental/build-out cost of the Multi-Agency Communications Center (MACC), the Coordinating Center and Credentialing Center.

The Secret Service will not be able to utilize the Presidential Assistance Act and therefore will not have access to military aircraft to transport vehicles, critical protective equipment and IT assets to this location. We will have to contract with a commercial vendor to transport these critical assets and ensure that they are available.

INFORMATION INTEGRATION AND TRANSFORMATION PROGRAM

Question. Provide a detailed crosswalk of the original modernization plan (schedule and budget) for the Information Integration and Transformation Program versus where we are with the program at current funding levels. Please detail any modernization funds that have been redirected for other purposes, including the amount and why they were redirected.

Answer. [The response is FOUO and Procurement Sensitive—See FAR 3.104 and the answer will be submitted under a separate cover.]

OPERATIONAL MISSION SUPPORT

Question. Please prioritize your Operational Mission Support requests (\$65 million).

Answer. Here is a list of the highest-priority operational mission support requirements. Each of these protective counter measures addresses a specific vulnerability or known threat that requires mitigation in order to provide a safe environment for the President and other national leaders. The protective counter measures are used individually and in combination to address specific types of threats, creating a high level of interdependence between the proposed systems. The counter measures provide enhanced security surveillance capabilities and defenses to known threats for the President at the White House and while traveling throughout the world. These assets will provide not only enhanced situational awareness capabilities, but also will enable notification systems to share critical information and activate emergency response protocols. They are listed below:

- Enhanced explosive detection systems, \$8,683,000 (51 positions).
- Enhanced chemical, biological, and radiological detection systems, \$4,626,000 (3 positions).
- White House physical protection upgrades, \$12,826,000 (3 positions).
- Enhanced White House camera system, \$6,375,000 (1 position).
- Development of next generation Presidential limousine, \$10,226,000 (3 positions).
- Presidential audio countermeasures, \$2,451,000 (2 positions).
- Cyber protection activities, \$12,775,000 (1 position).
- National master plan studies, \$1,375,000 (1 position).
- Protective systems and weapons testing program, \$6,477,000 (5 positions).

ANTICOUNTERFEIT OPERATIONS IN COLOMBIA AND PERU

Question. Please describe current anticounterfeit operations in Colombia and Peru. Has counterfeiting in Colombia decreased since the inception of the United States Secret Service cooperative presence with the Colombian Government? Is opening an overseas office in Peru under consideration?

Answer. [Follows:]

Colombia.—The U.S. Secret Service (USSS) Bogota Resident Office currently oversees the Vetted Anti-Counterfeit Force (VACF) composed of approximately 50 Colombian law enforcement officers divided among 8 offices in Bogota, Pereira, Cali, and Medellin. In addition, two Colombian district attorneys are exclusively working United States currency counterfeiting cases in conjunction with the VACF and USSS.

While overall statistics indicate steady attempts at counterfeit production within Colombia, the combined efforts of the USSS and Colombian VACF have been able to greatly reduce or interdict the export to, and subsequent passing of counterfeit within, the United States. Passing activity has decreased 81 percent since the inception of the USSS/Colombian cooperative anticounterfeiting effort.

Peru.—The Peru Counterfeit Task Force (PCTF) was formed in March 2009 and is currently working directly with the Peru National Police (PNP). The task force is composed of two agents on 2-week TDY assignment rotations. The USSS also started the process of selecting Peru National Police (PNP) officers with the goal of making a vetted anticounterfeit unit that closely mirrors the Colombian model. To date, PCTF efforts have led to the arrests of 50 suspects, the suppression of 22 counterfeit plant operations, and the seizure of more than \$36 million in counterfeit currency.

On February 15, 2011, DHS approved the National Security Decision Directive (NSDD) 38 related to the opening of the Lima, Peru office. On March 7, 2011, the NSDD 38 was officially submitted to the U.S. State Department. At this time, the USSS is awaiting review and approval from the U.S. State Department.

STATE AND LOCAL CYBER ACTIVITY

Question. President Obama has said, “the cyber threat is one of the most serious economic and national security challenges we face”. Secretary Napolitano, you included safeguarding and securing cyberspace as one of the five missions defined in the Quadrennial Homeland Security Review.

The fiscal year 2012 budget request appears to respond to this alarm by requesting a robust level of funding for US-CERT operations; Federal network security; and network security deployment. These are important areas to invest in and I take this request seriously. I was especially pleased to see that there is a \$9 million increase for outreach, education, and training activities. Many State, local, and private sector entities are struggling with and finding solutions to the same issues the Federal Government faces. Sharing solutions and expertise is imperative to our defense.

Please describe each cyber program underway that includes State and local efforts in fiscal year 2010, fiscal year 2011, and proposed programs for fiscal year 2012.

Further, what is the current status of cybersecurity and systems assurance curricula; and what capacity does DHS currently have to provide virtual education for specialized and classified education requirements?

Answer. The Department of Homeland Security’s (DHS) National Cyber Security Division (NCSD) collaborates with State, local, tribal, and territorial governments to share and implement sound cybersecurity policies, practices, and strategies to improve preparedness against cyber threats and attacks.

Due to the increasingly important role of State, local, tribal, and territorial governments in cybersecurity, NCSD has resources committed solely to interacting with officials at these levels. The mission of NCSD’s State, Local, Tribal, and Territorial (SLTT) Engagement program is to build partnerships with non-Federal public stakeholders, including each State’s Homeland Security Advisor, Chief Information Officer (CIO) and Chief Information Security Officer (CISO). The following provides an overview of NCSD interactions with States.

United States Computer Emergency Readiness Team

The United States Computer Emergency Readiness Team (US-CERT) maintains a formal relationship and works closely with mission partners, including State and local governments, on a daily basis to resolve threats, vulnerabilities, and incidents. US-CERT provides a variety of daily, weekly, monthly, and quarterly communication exchanges to maintain situational awareness and share critical information with collective cybersecurity partners. Federal and SLTT incident response personnel have access to the Government Forum of Incident Response and Security Teams (GFIRST) portal for information sharing and discussion.

US-CERT also sponsors the GFIRST National Conference, a forum that promotes cooperation among Federal agencies, State, local, tribal, and territorial governments, the private sector, and international partners across the cybersecurity spectrum, from preparedness and prevention to incident response. The conference supports the dissemination and promulgation of proactive and preventive security practices. US-CERT funding is executed toward planning, preparation, communication, and coordination of this conference and other conference expos. Specifically, \$1.55 million is directed to support requirements such as administration, logistics, and security. Additional funding (approximately \$3 million) provides support to the interactive demonstration system at the GFIRST National Conference.

US-CERT also provides support (\$1 million annually) to the Department of Commerce’s National Institute of Standards and Technology, which provides system integration and product development support for enhancement of the National Vulnerability Database and search engine. This database enables US-CERT partners, including State, local, tribal, and territorial governments, to secure government systems.

Multi-State Information Sharing and Analysis Center

Created in 2003, the Multi-State Information Sharing and Analysis Center (MS-ISAC) is an invaluable tool when dealing with SLTT governments. The MS-ISAC supports NCSD’s efforts to secure cyberspace by disseminating early warnings of cyber threats to SLTT governments. In addition, the MS-ISAC shares security incident information, identifies trends, and conducts other analysis for security planning. NCSD provides programmatic support (\$3.55 million for the 12-month period from August 1, 2010, to July 31, 2011) to the MS-ISAC. The fiscal year 2010 DHS

Appropriations Act provided an additional \$3 million for DHS to fund and work with the MS-ISAC to provide managed security services (e.g., intrusion detection systems, intrusion prevention systems firewalls) for 18 State and local governments. The MS-ISAC has selected State, county, and local governments for participation. The MS-ISAC, consistent with the objectives of NCSD, provides a common mechanism for raising the level of SLTT government cybersecurity readiness and response. It is a central resource for gathering information regarding cyber threats to critical infrastructure facilities. Other MS-ISAC programs/activities include:

Operation of a 24/7 Cyber Security and Analysis Center

The MS-ISAC runs a 24-hour watch and warning Security Operations Center (SOC) that provides real-time network monitoring, dissemination of early cyber threat warnings, and vulnerability identification and mitigation, along with education and outreach aimed at reducing risk to the Nation's SLTT government cyber domain. The SOC shares and coordinates real-time risk information to support national cybersecurity situational awareness with DHS (NCSD and US-CERT).

The SOC performs 24/7 monitoring of the Internet and other sources, including incident reports received from members and others regarding cybersecurity threats and vulnerabilities. The SOC staff evaluates and correlates information and distributes advisories and bulletins as appropriate, including mitigation strategies and steps that can be taken to protect critical infrastructure.

Managed and Monitored Security Services

The MS-ISAC contracts with the States of Alaska, Montana, and New York, along with the Los Angeles World Airports, to provide cybersecurity monitoring and managed services. This collective view across multiple entities helps enhance situational awareness regarding cyber threats.

During 2010, the MS-ISAC reviewed more than 78 billion logs through the 24/7 operations center. Approximately 138 MS-ISAC advisories were issued.

Additionally, through funding in the fiscal year 2010 DHS Appropriations Act, the MS-ISAC is expanding its monitoring services with an additional 10 State governments, 7 local governments, and 1 territorial government. This expanded infrastructure will provide a representative sample of system and network activity for enhancing situational awareness of SLTT government networks across the country. It will also improve cyber incident identification and response while providing more resources for developing and implementing appropriate mitigation strategies tailored specifically to SLTT government cyber resources.

Participation in Cyber Security Exercises—Cyber Storm I, II, and III

The MS-ISAC has participated in each of the three Cyber Storm exercises, most recently Cyber Storm III in September 2010. The MS-ISAC was a full player during the Cyber Storm III exercise; its SOC was active, and it coordinated with 11 States that participated in the exercise. The MS-ISAC hosted 19 visitors from five States, the Federal Bureau of Investigation, New York State law enforcement, Homeland Security and military personnel, and observers from the University of Texas at San Antonio.

National Cyber Incident Response Plan

The President's Cybersecurity Policy Review called for "a comprehensive framework to facilitate coordinated responses by Government, the private sector, and allies to a significant cyber incident." DHS coordinated the interagency, State and local government, and private-sector working group that developed the National Cyber Incident Response Plan (NCIRP). The Plan provides a framework for effective incident response capabilities and coordination among Federal agencies, State and local governments, the private sector, and international partners during significant cyber incidents. It is designed to be flexible and adaptable to allow synchronization of response activities across jurisdictional lines.

The NCIRP is undergoing final DHS review to incorporate lessons learned during the Cyber Storm III exercise. Upon conclusion of this review, DHS will send the NCIRP out to State, local and private-sector partners (including the National Governors Association and the MS-ISAC) for review. DHS will work with State and local partners (and partners in the private sector) to align their incident response plans and procedures with the NCIRP. The MS-ISAC and National Governors Association will be key partners in this effort.

DHS has designated the MS-ISAC as the ISAC for SLTT governments and has identified the MS-ISAC as a key stakeholder in the development and implementation of the NCIRP.

NCSD Cyber Security Evaluation Program

Under the 2009 appropriations act, NCSD's Cyber Security Evaluation Program (CSEP) was tasked with completing a Nationwide Cyber Security Review (NCSR). The NCSR is a voluntary self-assessment of State and major urban area government information technology (IT) services and is designed to measure cybersecurity preparedness and resilience. Through the NCSR, CSEP examines relationships, interactions, and processes governing IT management and the ability to manage operational risk effectively. CSEP also conducts voluntary cybersecurity assessments to evaluate and enhance the implementation of key cybersecurity capacities and capabilities of critical infrastructure and key resources (CIKR) sector members. This assessment is the Cyber Resilience Review, which is designed for each of the 18 CIKR Sectors and for use within SLTT governments. Since fiscal year 2009, CSEP has completed 45 cyber resilience reviews with SLTT partners.

NCSD Cyber Exercise Program

NCSD's Cyber Exercise Program (CEP) works with Federal, State, local, international, and private sector partners to conduct regional and sector-specific exercises designed to develop and improve the capabilities of DHS and its infrastructure partners. Such exercises aid participants in preparing for, preventing, mitigating, responding to, and recovering from cyber incidents. NCSD plans, coordinates, and conducts cyber exercises to develop, evaluate, improve, and refine the capabilities of State and local partners. CEP assists State and local partners by facilitating the design of tabletop and functional exercises at the State and local levels.

DHS hosted Cyber Storm III from September 26 through October 1, 2010. The Cyber Storm exercise series is a key element of ongoing efforts to assess cyber preparedness; examine incident response processes, procedures, and information sharing mechanisms; and identify areas for improvement absent the consequences of an actual incident. Cyber Storm III included participation from 11 States.

In 2009 and 2010, NCSD, the MS-ISAC, and the Microsoft Corporation jointly sponsored the Defend the Flag Exercises to provide State government network security professionals greater technical security skills and practical experience with implementing the principles of defense-in-depth while securing Windows-based operating systems. Thirteen States participated from 2009–2010.

Grants

DHS provides grants for cybersecurity through the Federal Emergency Management Agency (FEMA), such as the Homeland Security Grant Program (HSGP), which provides States the opportunity to work with DHS to acquire cybersecurity capabilities. During the last 2 years, NCSD has worked with FEMA to modify the language in the HSGP to better clarify how funds can be used to improve cybersecurity.

National Initiative for Cybersecurity Education

DHS is engaged in the National Initiative for Cybersecurity Education (NICE), leading Track 1 (Cybersecurity Awareness), leading Track 3 (Cybersecurity Workforce Structure), and coleading Track 4 (Cybersecurity Workforce Training and Professional Development). Through NICE, DHS is reaching out across the cybersecurity community—including academia, the private sector, and Federal, State, local, tribal, and territorial partners—to integrate current efforts into a foundation of information that creates mutual understanding and partnerships across all aspects of national cybersecurity.

In fiscal year 2010, DHS facilitated the efforts of six State government CIOs to develop a State government workforce development model, based on the existing DHS-issued Essential Body of Knowledge. This State government model was presented to the MS-ISAC, which included the model in its membership-based portal and on its public Web site.

Other NCSD SLTT Programs/Activities

National Cyber Security Awareness Month

To recognize the importance of cybersecurity awareness, October is designated as National Cyber Security Awareness Month. NCSD, with the help of the MS-ISAC, works with funded partners and other parties to sponsor events and activities throughout the country and disseminate Awareness Month key messages and event information to State and local partners. Due to the efforts of NCSD and MS ISAC, in 2009 and 2010, all of the Nation's governors signed letters officially proclaiming October as National Cyber Security Awareness Month.

Stop. Think. Connect. Campaign

DHS bears primary responsibility for raising public awareness about threats to the Nation's cyber systems and networks. To that end, in October 2010, DHS launched the National Cybersecurity Awareness Campaign, Stop. Think. Connect. It is a national public-education effort to engage and empower Americans to take charge of their online safety and security. By providing Americans with easy-to-understand online safety tips and resources, the campaign is helping them establish smart habits that will lead to increased protection online. Stop. Think. Connect. fulfills a key element of President Obama's 2009 Cyberspace Policy Review, which tasked DHS to develop a public-awareness campaign to inform Americans about ways to use technology safely.

Security Clearances for State Information Security Officers

NCSD, in partnership with colleagues from DHS Office of Security, initiated a plan to clear, starting at the secret level, each State CIO and CISO, and the MS-ISAC executive committee. NCSD is confident this is an important step in sharing valuable sensitive information with State partners.

Cyber Partner Local Access Plan

NCSD, in cooperation with the Office of Intelligence and Analysis, developed the Cybersecurity Partner Local Access Plan (CPLAP) to share classified cybersecurity threat information with cleared State cybersecurity officials and private-sector partners at State and major urban area fusion centers nationwide. The CPLAP enables more effective and efficient classified cybersecurity information sharing among Federal, SLTT, and private-sector partners, and supports an information-sharing model that eliminates partners' air travel to and from the Washington, DC, area to receive classified cybersecurity briefings. The CPLAP will be piloted at five fusion centers by mid-2011, with plans to expand the program to a broader audience and additional fusion centers on a regional basis by the end of 2011.

Cyber Summits

In an effort to educate SLTT leaders and the public, NCSD coordinates and plans Cyber Summits. These summits, which are held regularly throughout the year and hosted across the country, focus on opportunities and vulnerabilities to promote discussion on how public and private-sector officials can best leverage technology to reduce risk. Frequent attendance and contribution by nongovernmental cyber associations, such as the MS-ISAC and National Association of State Chief Information Officers, significantly contributes to the information sharing, capacity building, and coordination efforts necessary to develop robust and effective cybersecurity capabilities on all levels. DHS identified cybersecurity as a top departmental priority, and Federal, State, and local government officials share a responsibility to promote a healthy cyber ecosystem and to encourage individuals to protect themselves and their families at home, work, and school.

Virginia Operational Integration Cybersecurity Center of Excellence

NCSD is helping the Virginia Operational Integration Cyber Center of Excellence (VOICCE) create a Municipal Cyber Lab that will be used to support and train SLTT government officials to better understand cybersecurity issues. VOICCE focuses on incorporating cyber attacks into the mainstream of emergency operations at the local level and creating a virtual municipality of randomly generated Internet protocol addresses. The concept will allow for development of vital cybersecurity capabilities, processes, and procedures. The VOICCE node or laboratory will allow local governments and first responders to plug into State and Federal entities and participate in simulated cyber attacks. The lab will be both physical and virtual in structure, allowing many types of simulation and providing an effective environment to share ideas among stakeholders across the Nation. Participants will brainstorm, identify, and respond to diverse cyber attack scenarios.

This activity was required by the fiscal year 2010 DHS Appropriations Act.

NCSD will continue many of the programs listed above. In addition, in fiscal year 2012, NCSD will commit funding to expand the MS-ISAC's managed and monitor security services.

Curricula

The Software Assurance (SwA) curriculum project, which produced the Masters of Software Assurance (MSwA) curriculum and associated undergraduate course outlines, is a recent NCSD effort to cosponsor public-private collaboration for government, industry, and academia through its SwA Forum. To facilitate implementation, the MSwA project team is offering assistance, free of charge, to educational institutions looking to launch an MSwA degree program.

Through the Software Assurance (SwA) forum, the SwA program has encouraged Federal, State, and local involvement in public-private collaboration efforts associated with the advancement of SwA resources. As part of that collaboration, the SwA curriculum project released the Masters of Software Assurance (MSwA) reference curriculum and nine-course syllabi for public use. The MSwA curriculum is recognized by the Institute of Electrical and Electronics Engineers (IEEE) Computer Society and the Association of Computing Machinery (ACM) as the first curriculum of its kind to focus on assuring the functionality, dependability, and security of software and systems. The materials are available at <http://www.cert.org/mswa/>.

More information on the SwA curriculum project and the MSwA is available at <https://buildsecurityin.us-cert.gov/bsi/1165-BSI.html>.

Virtual Education

The SwA Forum, sponsored by NCSD's SwA Program, posts Web casts of SwA tutorials and pocket guides that are publicly available for free online use, including links via virtual training environments.

One aspect under NICE Track 4 is Functional Area 4, which concerns Specialized Cybersecurity Operations. The scope of this effort includes those Federal civilian employees, members of the uniformed services, and contractor personnel employed by departments and agencies who are engaged in highly specialized and largely classified cybersecurity operations. Work associated with this functional area is classified, but a classified briefing to discuss the work associated with this topic can be arranged upon request.

RISK ASSESSMENT PROCESS FOR INFORMED DECISION MAKING (RAPID)

Question. NPPD began development of the Risk Assessment Process for Informed Decision Making (RAPID) to aid the Department in making policy and budgetary decisions based on risk. Which DHS components (or other entities) have used RAPID to date? What impact did it have on operations? What proposals in the fiscal year 2012 budget used RAPID as the foundation for the request? What is the next phase for RAPID and when will it be used departmentwide?

Answer. [Follows:]

Components That Have Used RAPID to Date

The Risk Assessment Process for Informed Decision Making (RAPID) is the Federal Government's first quantitative, multi-mission, multi-hazards assessment of homeland security risk. RAPID assesses the risk of various types of terrorism, natural disasters, and transnational crimes in terms of annualized expected fatalities and economic losses. The goal of RAPID is to provide information about these homeland security risks and the extent to which Department of Homeland Security (DHS) programs and activities contribute to the reduction of these risks to support DHS leadership decisionmaking during the annual planning, programming, budgeting and execution (PPBE) process cycle and supporting processes.

To date, RAPID analysis has supported the planning phase of the annual DHS PPBE cycle through the development of the Office of Policy's Integrated Planning Guidance by highlighting key risks and providing qualitative analysis of possible risk-mitigation strategies. In addition, RAPID analysis has proven helpful in facilitating more robust evaluation of alternatives within the Program Review Board issue teams.

In addition to supporting the departmentwide PPBE process, RAPID has supported a number of DHS components in prioritizing their activities, as described below.

United States Coast Guard Ports, Waterways, and Coastal Security Program

The United States Coast Guard's (USCG's) Ports, Waterways, and Coastal Security (PWCS) Risk-Based Performance Module has been developed to:

- Assess risk in the PWCS mission;
- Evaluate USCG performance within the mission; and
- Evaluate the effectiveness of USCG planning, programming, and budgeting recommendations in terms of risk reduction.

To achieve those objectives, the model considers a wide array of maritime terrorism scenarios. The risk data for the vast majority of scenarios comes directly from the USCG's Maritime Security Risk Analysis Model; however, the risk of transferring terrorists and Weapons of Mass Destruction (WMDs) through the maritime domain is currently outside of the model's scope.

To establish the risk associated with these scenarios, the USCG/PWCS team requested RAPID data from the National Protection and Programs Directorate's (NPPD's) Office of Risk Management and Analysis (RMA) related to the following:

- Frequency estimates from RAPID’s structured elicitation of the intelligence community in the following areas:
 - Maritime-related WMD transfers, both through ports of entry and between ports of entry;
 - Maritime-related terrorist transfers, both through ports of entry and between ports of entry;
 - Maritime-related direct attacks; and
 - Maritime-related direct exploitation attacks.
- Casualty and economic consequence estimates for a variety of WMD attacks.

DHS Office of Policy’s Office of Strategic Plans

The Office of Strategic Plans within the Department’s Office of Policy requested information and analysis related to:

- The overall flows of four types of drugs that malefactors are attempting to introduce into the United States;
- Estimates of drugs seized based on the reported sources; and
- How these reported estimates compare with RAPID estimates.

In response to this request, RMA provided overall drug-flow estimates, as well as drug-seizure estimates from both RAPID and other reported sources.

Immigration and Customs Enforcement Homeland Security Investigations

In response to the Government Accountability Office report, “Better Management Practices Could Enhance DHS’s Ability to Allocate Investigative Resources” (GAO-06-462T), the Immigration and Customs Enforcement (ICE) Homeland Security Investigations has been seeking a way to use risk management to inform its resource allocation decisions (i.e., analyze its primary enforcement areas and allocate its resources according to the likelihood of potential consequences to the United States). As a result, ICE developed a strategic risk assessment whose methodology was peer-reviewed at multiple stages by RMA, and RMA provided RAPID analysis for use in this assessment. Specifically, RMA provided RAPID analysis of residual drug-flow estimates, consequences as a result of foreign-produced drugs, and consequences due to illegal migration. ICE used the RAPID data to augment and validate its own estimates.

Customs and Border Protection Agro/Bio-Terror Countermeasures

RMA has been asked by Customs and Border Protection’s (CBP’s) Agro/Bio-Terror Countermeasures (ABTC) to provide bioterrorism/agroterrorism risk information to inform its targeting processes. Specifically, ABTC is interested in using RAPID in the following areas:

- Assist in improved use of targeting resources by either:
 - Using existing RAPID risk results tailored to provide information regarding risk by “mode and point of entry” for biological material to inform ABTC’s decisions regarding the allocation of its resources among air, land, and sea border crossings; or
 - Building a new “risk factor” category into ABTC’s existing targeting rulesets that includes RAPID “mode and point of entry” risk data; and
- Help design probabilistic red-team scenarios to test targeting and response procedures.

Impact on Operations

As noted in the Secretary’s policy statement on Integrated Risk Management signed in May 2010, DHS uses risk information and analysis:

“ . . . to inform decisionmaking, striving to better understand risks and capabilities to manage them, while remaining flexible to changing risks. Homeland security risks are inherently uncertain, and risk analysis will not always yield precise answers. The Department uses risk information and analysis to make its assumptions more transparent, encourage creative thinking, and provide defensible decisions, made with the best available tools and information, for the best achievable outcomes.”

Using risk analysis to inform decisions, particularly operational ones, is a complicated process that involves making difficult tradeoffs among often highly uncertain risk reduction benefits, costs, the unique risk tolerance of the decisionmaker, logistical constraints, and policy priorities. Terrorism risk analysis in particular involves a great deal of uncertainty that affects our ability to estimate the range of potential benefits of different alternatives.

Fiscal Year 2012 Proposals That Used RAPID as the Foundation for the Request

During the fiscal year 2012 budget build, RAPID was not completed in time to serve as the foundation for any specific budget requests. It is expected in the future,

however, that RAPID will reach a sufficient level of maturity to be leveraged more broadly and will increasingly provide greater input into the budgeting process.

Next Phase for RAPID

Following the execution of RAPID 2010, NPPD/RMA conducted a formal lessons-learned process to prioritize enhancements to future iterations of the assessment. This process led to a formal confirmation of strategic requirements and reinforced the focus for RAPID in 2011–2012 to better understand customer needs and the decision environment. Initial RAPID 2010 analysis provides a baseline view of homeland security risk and risk reduction across the Department's mission-oriented programs, portfolios, and activities. In 2011, RMA plans to invest most of its effort in improving model and data quality, bringing all RAPID analysis in house so that it can be conducted by Federal staff on Federal computing equipment, and conducting tailored analysis to support the fiscal year 2013–2017 budget build, including support to NPPD's budget request, study of the effectiveness of chemical, biological, radiological, and nuclear countermeasures, and more effective allocation of aviation security and air domain awareness resources.

PROGRESS IN INTEROPERABILITY

Question. The 10th anniversary of the terrorist attacks on September 11, 2001, is only 6 months away. The failure of communications during that incident has been cited in the 9/11 Commission report and has been the subject of many recommendations for improvement. During Hurricane Katrina, we once again witnessed a failure in communications during a catastrophe. The Federal Government and the Department of Homeland Security have devoted significant resources to solving the interoperable communications problem; more than \$4.5 billion in Federal homeland security grants alone. State and local governments have contributed an untold amount. Progress has been made; however, interoperable emergency communications remain inadequate.

The emergence of broadband services provides emergency responders with new opportunities to improve communications. Despite this potential, public safety officials face several challenges in integrating new technologies and proving their reliability. What progress has been made since September 11, 2001, to improve emergency communications and what challenges lie ahead? Does the National Emergency Communications Plan need to be updated for emerging technologies and services? What is the plan to develop and disseminate training and best practices on governance, standard operating procedures, equipment purchases, and related issues for emerging technologies and services and to deliver technical assistance to public safety agencies on broadband technologies?

Answer. [Follows:]

Progress Made Since September 11, 2001

Improving communications for the Nation's emergency responders has been a top priority for the Department of Homeland Security (DHS). Since its establishment, DHS has worked with its partners at the Federal, State, local, tribal, and territorial levels to build and sustain the communications capabilities that public safety personnel require at all times to coordinate response and recovery operations effectively. Creation of the Office of Emergency Communications (OEC) within the National Protection and Programs Directorate in 2007 and its subsequent release of the National Emergency Communications Plan (NECP) have been key drivers of progress in this mission. To date, the Department has achieved 78 of the 92 milestones in the NECP, or 85 percent.

The Office for Interoperability and Compatibility (OIC) within the Science and Technology Directorate (S&T) was created in 2004 to strengthen and integrate interoperable communications. Working closely with the emergency response community, OIC developed foundational tools, methodologies, and standards to strengthen interoperability. For example, OIC improved command-level interoperability capabilities in 10 high-threat urban areas through the RapidCom initiative. OIC also supported RapidCom 2 which accelerated the completion of Tactical Interoperability Communications Plans in the largest 75 urban/metropolitan areas across the Nation. A scorecard was developed to help all levels of government measure their current state of interoperability and lay the foundation for establishing accountability for future progress. Additionally, OIC launched two regional communications interoperability pilots in Nevada and Kentucky which resulted in guidance documents on governance, funding, and procurement that now serve as tools for States and territories in support of their statewide planning efforts.

Prior to the creation of OEC and release of the NECP, emergency response agencies often pursued disparate emergency communications activities and lacked coordi-

nated solutions and protocols. Few plans existed at the State level to guide activities within or across States and with Federal efforts, and inter-agency coordination at the Federal level was not as effective as it needed to be. In addition, Federal grant programs supported the acquisition of communications equipment—but without common governance and statewide plans in place, individual communities often made equipment investments without coordinating with their neighboring communities or regions.

To address these and other interoperability challenges, OEC developed the NECP in coordination with more than 150 representatives from all major emergency response organizations across the country, including the SAFECOM Executive Committee/Emergency Response Council, Federal departments and agencies through the Emergency Communications Preparedness Center (ECPC), and private-sector and nongovernmental organizations. The NECP set out a clear strategy for building capabilities in key areas identified by public safety as needed for improving emergency communications and has since greatly influenced planning, governance, operating procedures, and training for responders nationwide.

Indicators of Emergency Communications Progress

NPPD/OEC's efforts to coordinate with stakeholders from the Federal, State, local, tribal, and territorial responder communities and the private sector to improve interoperable emergency communications capabilities have resulted in:

- Enhanced Statewide Coordination.*—The creation of 56 statewide Communication Interoperability Plans (SCIPs) and 44 Statewide Interoperability Coordinators (SWICs) is improving coordination of emergency communications activities and investments throughout all 56 States and territories. All 56 States and territories have identified a point of contact for statewide interoperability coordination, and 44 States and territories have full-time SWIC or equivalent positions. These important leadership roles and planning mechanisms are critical for the continued funding, accountability, and execution of emergency communications activities at the State, local, tribal, and territorial levels.
- Common Plans and Procedures.*—The creation and increased use of standardized plans, protocols, and procedures is driving improved command, control, and communications among emergency response agencies in the field. NPPD/OEC and the Federal Emergency Management Agency (FEMA) have worked with more than 140 jurisdictions to develop Tactical Interoperable Communications Plans (TICPs) that document formalized interoperability governance groups, standardized policies and procedures, and emergency communications equipment inventories. DHS continues to work with stakeholders to update, implement, and develop new TICPs as part of the NECP. In addition, more than 30 States are implementing plain-language protocols to simplify and standardize the language used to share information and communicate during an emergency.
- Targeted Technical Assistance.*—As part of the NECP, NPPD/OEC has implemented a technical assistance strategy to ensure that all States and territories can request and receive emergency communications assistance while also focusing support on the States and urban areas most in need. This technical support provides improvements in all areas of emergency communications, including the development of governance structures, tactical and strategic planning, and a variety of engineering services. Since 2008, the 56 States and territories have requested more than 750 individual technical assistance services from NPPD/OEC. These services support the priorities in each State or territory's SCIP and the objectives of the NECP.

The 2011 Technical Assistance Catalog has 13 new or updated offerings to provide support to States across the entire Interoperability Continuum, one of which is focused on the planning for and incorporation of 700MHz Wireless Broadband technologies into the Public Safety community. In addition, NPPD/OEC is conducting at least five focused Technical Assistance engagements with jurisdictions granted waivers by the Federal Communications Commission for conditional use of currently allocated 700 MHz spectrum to help them migrate to the new 700MHz Long-Term Evolution network and share best practices with the Nation. Last, NPPD/OEC facilitates a weekly call with the Public Safety Spectrum Trust Operator Advisory Committee, a group comprising all the jurisdictions receiving such FCC waivers, to encourage information sharing and collaboration.

- Increased Training Opportunities.*—To improve emergency responders' capabilities in this area, OEC's Communications Unit Leader (COML) training program has resulted in the training of more than 3,500 responders, technicians, and planners to lead communications during incidents across the Nation, including local floods, blizzards, and wildfires. Effective training and exercise programs

can increase emergency responders' proficiency with equipment and help them coordinate roles and responsibilities more effectively during an event. Trained COMLs also contributed to recovery efforts outside of the United States, such as the response to the 2010 earthquake in Haiti.

—*Improved Governance and Coordination.*—Building on the success of governance and coordination mechanisms such as the SAFECOM Executive Committee/Emergency Response Council, NPPD/OEC has worked with Federal, State, local, tribal, and territorial agencies to stand up formal decisionmaking structures that increase coordination, information sharing, and oversight of interoperability:

—Statewide Interoperability Governing Bodies now exist in every State and territory and include representatives from all levels of government to coordinate and support statewide interoperability. In addition, many States have created regional interoperability committees to provide insight into the statewide strategy from an operational perspective.

—NPPD/OEC established the National Council of Statewide Interoperability Coordinators to serve as a governing body for SWICs. The council meets twice a year to share best practices, lessons learned, successes, and challenges related to SCIP implementation.

—DHS established Regional Emergency Communications Coordination Working Groups and placed individual regional coordinators from FEMA, NPPD/OEC, and the National Communications System in each of the 10 FEMA regions to coordinate interstate emergency communications efforts.

—The Emergency Communications Preparedness Center represents the Federal Government's broad role in emergency communications, including regulation, policy, operations, and grants. The ECPC, which comprises members from 14 Federal departments and agencies, is driving more effective coordination of grants, technical assistance, and planning activities for emergency communications.

NECP Goals Performance Measurement.—The NECP goals serve as performance benchmarks for assessing public safety agencies' progress toward achieving a baseline-level of interoperable emergency communications. OEC is measuring them through a process that engages Federal, State, local, tribal, and territorial emergency responders. The three NECP goals are as follows:

Goal 1.—By the end of 2010, 90 percent of all high-risk urban areas designated within the Urban Areas Security Initiative (UASI) can demonstrate response-level emergency communications within 1 hour for routine events involving multiple jurisdictions and agencies.

Goal 2.—By the end of 2011, 75 percent of non-UASI jurisdictions can demonstrate response-level emergency communications within 1 hour for routine events involving multiple jurisdictions and agencies.

Goal 3.—By the end of 2013, 75 percent of all jurisdictions can demonstrate response-level emergency communications within 3 hours of a significant event, as outlined in the department's national planning scenarios.

—To evaluate NECP goal 1, NPPD/OEC conducted an assessment of response-level emergency communications among public safety agencies during a planned event held in each UASI region. Based on the interoperable communications capabilities documented at each event, all 60 UASI regions were able to demonstrate response level communications, achieving NECP goal 1. The goal 1 assessments also identified areas for continued improvement. NPPD/OEC will use the results of the goal assessments—including goal 2, scheduled for completion in 2011 and goal 3, scheduled for completion in 2013—to better target resources, such as training and planning, for improving interoperable emergency communications nationwide.

Updating the National Emergency Communications Plan

NPPD/OEC is leading efforts to update the NECP to address the integration of broadband with traditional Land Mobile Radio (LMR) technologies. OEC is coordinating with Federal, State, local, tribal, and territorial agencies, major public-safety organizations, and the private sector to develop a strategy for incorporating new technology, such as broadband, while maintaining the mission-critical voice-over LMR that responders use every day to save lives. The NECP update will focus on key issues that must be addressed, such as partnerships, planning, user requirements, standards, research and development, and funding.

Acceleration of Standards and Technology Developments

OIC has worked to provide stakeholders (local, State, and Federal), with the optimal mix of standards, tools, technologies, methodologies, and guidance to enable im-

proved communications interoperability at all levels. For example, OIC facilitates the development of Emergency Data Exchange Language (EDXL) standards through a practitioner-driven approach. These standards enable the emergency response community to share data seamlessly and securely during an incident. Once standardized, any technology vendor or organization can easily develop EDXL-based applications and products to facilitate information exchange across disparate public safety systems across local, tribal, State, Federal, and nongovernmental emergency response and management disciplines. The EDXL family of standards is developed through input from the OIC-Sponsored Practitioner Steering Group (PSG) and Standards Working Group (SWG). The PSG and SWG represent multiple disciplines, ensuring that the requirements reflect an all-hazards perspective. The standards are then vetted by an international standards development organization. The EDXL project is a public-private partnership established to create an information sharing capability between disparate emergency response software applications, systems, and devices.

An example of the Department's promotion of voice standards is OIC's Project 25 Compliance Assessment Program (P25 CAP), which established a process for ensuring that emergency communications equipment complies with P25 standards and is capable of interoperating across manufacturers. P25 standards make it possible for radios to interoperate regardless of manufacturer, enabling emergency responders to communicate. Currently, P25 CAP has 12 participating manufacturers, representing more than 80 percent of the land mobile radio market. The program, a partnership between DHS S&T and the National Institute of Standards and Technology, provides local, State, and Federal emergency responders with an independent and transparent process to formally assess communications equipment against a select group of requirements within the suite of P25 standards. The results from this testing are published on FEMA's Responder Knowledge Base Web site. The P25 CAP will allow emergency responders to purchase and use P25-compliant products.

Recognizing the emergency response community's need for standards-based, Internet protocol-enabled backbones that improve mission-critical information sharing and allows for the interconnection of Voice over Internet Protocol (VoIP) based networks with neighboring agencies, OIC established a Public Safety VoIP Working Group. This Working Group, consisting of public safety practitioners, industry representatives, and Federal partners, created the Bridging System Interface (BSI) core profile. The BSI allows emergency response agencies to seamlessly connect radio systems over an IP network—regardless of the manufacturer. Thirteen manufacturers voluntarily adopted the BSI platform and others have committed to doing so in their next product cycle. Ultimately, the BSI core profile provides emergency response agencies with a reduction in cost for system design and installation.

The introduction of Multi-Band Radio (MBR) technology to the emergency response community offers an opportunity to improve interoperability across agencies, disciplines, and jurisdictions by providing the capability to communicate on all public safety radio bands. OIC's MBR technology project evaluates, tests, demonstrates, and pilots MBR technology to ensure that equipment meets the mission requirements identified by the emergency response community. Finally, compiling the data and user feedback from the test and evaluation phases, OIC will produce a detailed procurement guide that will assist emergency response agencies in the identification of equipment functionality offered by various manufacturers that meets their radio communication interoperability requirements. DHS believes that their efforts with this project will continue to stimulate the marketplace and encourage additional manufacturers to research, develop, design, and manufacture similar technology.

OIC also developed a Technology Roadmap for Interoperable Communications to provide stakeholders with a strategy to incorporate new and emerging technologies into existing communications capabilities.

Broadband

DHS is deeply involved in coordinating public-safety broadband efforts at the Federal, State, local, tribal, and territorial levels. NPPD/OEC is helping to set the broad policy framework for public-safety broadband networks and ensuring that it aligns with existing emergency communications policy. NPPD/OEC is offering technical assistance to the jurisdictions that received FCC waivers to allow early deployment of broadband public safety facilities and other early adopters of broadband solutions to ensure that their activities remain aligned with the vision of a nationally interoperable network. NPPD/OEC is also developing guidance documents geared toward elected officials, SWICs, and UASI/regional coordinators within a State to provide an overview of broadband technology, guidance on interoperability planning for broadband, best practices from the waiver jurisdictions, and regional governance considerations. NPPD/OEC is also coordinating Federal broadband efforts to develop

requirements and influence standards associated with potential Federal user participation in the National Public Safety Broadband Network.

PRIVATE SECTOR COORDINATION AND INFORMATION SHARING

Question. NPPD has various methods for coordinating and sharing information with the private sector related to critical infrastructure. The fiscal year 2012 budget proposal indicates that NPPD will streamline the process. Please provide a list of each coordination group (i.e. national infrastructure protection plan management, critical infrastructure key resources coordination, sector-specific agency management); their authority or reason for creation (law, regulation, Presidential directive, department initiative); how often each group meets; and what each produces or accomplishes. Please describe in detail how the fiscal year 2012 budget will streamline the current process and how it will be coordinated with the private sector coordination office in FEMA.

Answer. The following chart lists each coordination group, authority, engagement frequency, products/accomplishments, and membership. In addition, the Partnerships project has tracked the following growth in the use of the National Infrastructure Protection Plan (NIPP) partnership structures:

	Fiscal year 2008	Fiscal year 2009	Fiscal year 2010
Partnership member institutions	492	643	861
Partnership councils and working groups	57	78	79
Individual meeting participants	1,530	1,723	2,197
Council and working group meetings	258	475	628

CRITICAL INFRASTRUCTURE COORDINATION GROUPS

Organization	Authority	Engagement frequency	Products and accomplishments	Membership
Education, training and outreach awareness working group.	National Infrastructure Protection Plan (NIPP).	Meets three times per year	Information sharing with sector-specific agencies (SSAs) on education, training and outreach activities.	DHS and SSAs
IP-SSA biweekly coordination call	Department initiative supporting HSPD-7, NIPP.	Occurs every other Thursday	Regular communication and coordination mechanism between IP and the SSAs to discuss ongoing initiatives and issues.	SSA representatives
Risk Management Enhancement Initiative Working Group.	Department initiative supporting HSPD-7, NIPP.	Monthly	Supports the development of the improved NAR/SARs/metrics, the new Critical Infrastructure Risk Management Plan (CIRMP), and the National Risk Profile (NRP).	SSA representatives
North American Electric Reliability Corp (NERC) Pilot Program.	Supports NIPP and HSPD-7 reporting requirements.	Ad hoc	Provides insight into measuring and evaluating resilience within the electric industry.	DHS, NERC
Sector Annual Report/National Annual Report (SAR/NAR) technical assistance sessions (for each sector-specific agency).	Supports NIPP and HSPD-7 reporting requirements.	Annually	Meetings are conducted at the beginning of the SAR/NAR reporting cycle in order to discuss sector writing, development, and metrics guidance as it applies.	DHS, SSA representatives
SLITGCC and RCCC technical assistance sessions.	Supports NIPP and HSPD-7 reporting requirements.	Annually	Meetings are conducted to discuss SLIT writing, development, and metrics guidance.	DHS, SLITGCC, RCCC representatives
Federal Senior Leadership Council meetings.	HSPD-7, NIPP	Quarterly	Cross-sector coordination	SSA leadership or their representatives
CIMR Cross-Sector Council meetings	HSPD-7, NIPP	Quarterly	Cross-sector coordination	SCC leadership
Agriculture and food sector	HSPD-7, NIPP	Each quarterly at minimum	Various sector products (Annual report, sector roadmaps, etc.).	SCC: Trade Associations and Owner/Operators GCC: government representatives
SCC meetings				
GCC meetings				
Joint SCC, GCC, CIPAC				
Banking and finance sector	HSPD-7, NIPP	Each quarterly at minimum	Various sector products (Annual report, sector roadmaps, etc.).	SCC: trade associations and owner/operators GCC: government representatives
SCC meetings				
GCC meetings				
Joint SCC, GCC, CIPAC				

Regarding the fiscal year 2012 budget, information sharing and coordination activities for the National Protection and Programs Directorate's Office of Infrastructure Protection (IP) planned for fiscal year 2012 are designed to improve the effectiveness and coordination of the councils and expand the participation in information-sharing activities by critical infrastructure stakeholders. One key aspect is enhancing the critical infrastructure information sharing environment and the use of the Homeland Security Information Network-Critical Sectors.

NPPD/IP routinely coordinates with the Federal Emergency Management Agency's Private Sector Division and others, especially related to training and education activities that are appropriate for the full private-sector community. In addition, NPPD/IP, in coordination with the Department of Homeland Security's Private Sector Office and the Office of Intelligence and Analysis, began a private-sector information-sharing improvement initiative in the spring of 2010. The initiative focuses on adopting a "One DHS" private-sector information-sharing approach and seeks to:

- Enhance strategic communications coordination;
- Strengthen regionally focused information-sharing efforts; and
- Enhance information sharing and accountability.

Through this initiative, DHS will work to increase coordination with interagency private-sector information-sharing efforts, evaluate and enhance existing processes and methods of information sharing with critical infrastructure owners and operators, and improve cross-sector information visibility and collaboration within the Critical Infrastructure Key Resources Information Sharing Environment. All DHS components with private-sector information-sharing activities are participating in this initiative.

FEDERAL PROTECTIVE SERVICE WORKFORCE ANALYSIS

Question. Recent events demonstrate that Federal employees are at greater risk. The Federal Protective Service (FPS) is charged with protecting employees on Federal property from those who threaten harm to the workforce. Yet, FPS has struggled with providing optimal service. Balancing its workforce needs against risk is critical to ensuring FPS evolves into a premier agency. Senate Report 111-222, accompanying the Department of Homeland Security Appropriations Bill, 2011 directs the National Protection and Programs Directorate to provide a workforce staffing model to the subcommittee and to the General Accountability Office (GAO) within 45 days. To date, the staffing model as not been provided. Please provide a copy of the staffing model to the subcommittee and to GAO.

Answer. The National Protection and Programs Directorate prepared a Federal Protective Service staffing plan which is currently being finalized.

US-VISIT—CARRYOVER BALANCES

Question. A portion of the fiscal year 2012 budget request assumes that a significant level of carryover balances of prior year funds will be available to hire staff and perform other activities.

What impact will there be on US-VISIT if the assumed carryover balances are not available for these intended purposes? What changes to the program or to US-VISIT operations will have to be made?

Answer. In this fiscally constrained environment, some difficult choices had to be made—one of which was to use the \$25.642 million as an offset to provide funding for other departmental priorities. Looking towards fiscal year 2012, a realignment of funds will be necessary in order to enhance the collection and use of biographic exit data and the review of potential overstay records—both of which will increase our current capabilities and lay a strong foundation for other exit measures in the future. The President's budget proposes the realignment of \$24.358 million in carryover balance in order to hire temporary staff to eliminate the existing overstay backlog, as a prerequisite for any future biometric exit capability. If the carryover balances were not available for this purpose, US-VISIT will not be able to clear the existing backlog.

FEDERAL EMERGENCY MANAGEMENT AGENCY (FEMA)—DISASTER RELIEF

Question. The Disaster Relief Fund (DRF) provides financial support for both response and recovery in States that are overwhelmed by the devastation of a disaster. For fiscal year 2011, we are facing a \$1.6 billion gap in the DRF. If the President does not request and the Congress does not approve supplemental funding, the account will run out of money in June, just as we are entering the hurricane season. For fiscal year 2012, the problem is even worse because we are facing a \$3 billion gap between the President's request and the known costs of past disasters. These shortfalls are specifically the result of past major disasters, such as Hurricanes

Katrina, Rita, Gustav, and Ike, the Midwest floods of 2008, and the Tennessee floods of 2010.

In fiscal year 2010, there was a similar shortfall. FEMA had to stop providing assistance for rebuilding and recovery projects to ensure it had enough for immediate needs for disaster response to new events. For 5 months, recovery projects all over the Nation stopped. In this economy it was not welcome news. Plus, the delays only make the projects more expensive.

Unfortunately, history is repeating itself.

Please provide a report with quarterly estimates of funding requirements for the DRF for the current fiscal year, fiscal year 2012, and fiscal year 2013. The report should include an estimate for the costs of all previously designated disasters by quarter; the cost of future disasters based on a 5-year average, excluding catastrophic disasters, by quarter; and a projected date on which the DRF will reach a balance of \$500 million.

When will the President submit an emergency supplemental request for the known shortfalls?

In lieu of a supplemental request, the House responded to this shortfall by cutting \$1.6 billion out of the base Homeland Security budget in H.R. 1. They cut the Coast Guard. They cut FEMA. They cut grants to State and local first responders and emergency managers. Do you believe the House approach to funding the shortfall is the right approach?

If we do not receive an emergency supplemental request, what specific cuts will the President propose below his requests for fiscal year 2011 and fiscal year 2012 to pay for this shortfall? Or is it your policy that FEMA should do what it did last year and simply stop making recovery payments?

Answer. The \$1.8 billion requested for the DRF, per standard annual practice, reflects the 5-year rolling average of historical obligations for noncatastrophic events (those less than \$500 million in estimated obligations), less estimated recoveries for fiscal year 2012. This methodology is one that the administration has proposed in its fiscal year 2010 and fiscal year 2011 budgets and represents the best use of available information in developing the DRF request. We also have a robust strategy in place to deobligate funds from past contracts and projects that are now complete and where we did not spend all the money originally obligated. Based on our experience in actively managing the unliquidated contract obligations in fiscal year 2010, we are taking the same approach for Individual Assistance and Public Assistance grants in fiscal year 2011, and anticipate that our projected recoveries may be higher than previously estimated. Regardless, we are committed to working with the Congress to ensure that the DRF remains solvent through fiscal year 2011 and fiscal year 2012.

PROPOSED CUTS TO FEMA

Question. I am very pleased to see that you have taken a hard look at the budget and found places to save on administrative cost such as travel and supplies. While I encourage you to continue to find ways to create efficiencies, I am concerned that some areas go beyond efficiencies and become deep cuts that inhibit performance.

The fiscal year 2012 budget proposes a \$68 million cut to FEMA's Management and Administration account (including all transfers). No other component in the Department was subjected to such a significant cut to its base operations. This proposal looks like the beginning of a trend of previous cycles that FEMA has been through. In tough budget times and when major disaster responses are a distance memory—at least for some inside the beltway—we trim back our readiness efforts.

The budget proposal cites cuts to facility improvements, information systems, and communications systems. Deferred maintenance of facilities, turns into deferred maintenance of programs, turns into deferred capabilities. Unfortunately, this has not worked well in the past.

In fact, there are a series of reports that show a disturbing cycle of building up an emergency management capacity after a failed disaster response, letting the capacity wither away when there hasn't been a major event for awhile, and then building the capacity back up again after another failed response.

For example, in 1983, a GAO report found that FEMA suffered from a variety of management and program problems. Ten years later and after the devastation of Hurricane Andrew, the National Academy of Public Administration—citing the 1983 GAO report—found many of the same problems. Twelve years after Hurricane Andrew, a myriad of reports found that the very same problems crippled the response to Hurricane Katrina.

Immediately after each of these disasters, FEMA improved only to devolve again within a 10-year period. This is a costly way to do business.

This subcommittee has done its part to ensure the resources FEMA needs to rebuild itself once again have been provided since Hurricane Katrina. Since 2005, FEMA's workforce has been increased by 50 percent to 4,700 strong. Catastrophic planning is more integrated among the levels of government. Shelter facility data is better managed between the public and private sectors. The disaster contract acquisition process is now proactive, not reactive.

But we have to maintain these improvements. And we still have serious work to do—FEMA is not done rebuilding itself. The national disaster recovery framework has not been completed; an effective risk and preparedness assessment system is not in place; FEMA information systems are not sufficient; and the human resources study is not complete.

While not all of these are big expenses, each effort requires a strong FEMA base. I am afraid this budget marks the beginning of letting FEMA wither on the vine again—just as it did before Hurricane Katrina.

Please provide a complete breakdown of the cuts by FEMA component, an explanation of the impact, and a distinction between which cuts are onetime costs from fiscal year 2010 and which cuts will delay programs and by how long. Why are you satisfied that FEMA can sustain such cuts and not only maintain its recent improvements but also keep pace with evolving risks?

Answer. The fiscal year 2012 President's budget provides the resources required to support the Agency's ability to fulfill its emergency management mission. In light of the current fiscal climate and through pursuit of identified efficiencies, FEMA cut administrative costs and professional services contracts by streamlining current business processes, harnessing the use of innovative technologies, and eliminating nonmission-critical spending in order to preserve essential operational activities.

For example, the proposed decrease of \$1.6 million in fiscal year 2012 to FEMA's Office of the Chief Component Human Capital Officer (OCCHCO) programs in the Management and Administration (M&A) account will not adversely affect the regional offices' abilities to handle the expected workloads with regard to hazard mitigation or grants management activities, nor does the decrease directly affect any staffing levels in the agency.

Specifically, \$900,000 of the decrease represents the elimination of funding for the Building Engagement, Strengths, and Talent (BEST) contract. FEMA found that the data garnered from the BEST surveys and analysis is available from other agency workforce development data sources.

The balance of the budget cuts are split equally between the following three areas:

- Finding general operational efficiencies within less costly general operational requirements, such as enhanced use of video teleconferencing vs. travel expenditures;
- Leveraging training cost savings by deconflicting separate but similar agency training offered in the separate FEMA Qualification System training programs; and
- By shifting contract support costs, which directly support the disaster workforce, to the DRF appropriation.

The proposed funding in the fiscal year 2012 budget request supports robust oversight of emergency management operations; national-level exercises to test FEMA's ability to respond to a catastrophic cyber attack; the development of catastrophic plans focused on response to biological events and earthquakes; and emergency preparedness, coordination, and planning at the local level.

The following chart provides the requested information. Unless otherwise noted, all cuts are reoccurring.

FISCAL YEAR 2012 MANAGEMENT AND ADMINISTRATION REDUCTIONS

[Dollars in Thousands]

Directorate/office	Fiscal year 2011 to fiscal year 2012 reductions	Impact statement
Office of Response and Recovery (ORR)— Front Office: Disaster Management Support Environment (DMSE).	(2,690)	FEMA will move as much of the activity as possible to other sources of funding, leveraging the assistance of DHS S&T, and sharing the burden across applicable appropriations.
Response: Travel	(2,645)	While mission-critical travel will not be affected, this cut will reduce general and conference attendance by leveraging Web conferencing and other technology tools.
Contracts	(5,562)	In-source several Directorate-wide contracts and convert on-site contractor support positions to FTEs.
Recovery: Travel	(812)	Eliminate nonmission-critical travel; maximize use of conference calls and Web-based training and meetings.
Contracts	(6,578)	Reduce selected projects funding through efficiencies.
Equipment	(454)	\$453,800 reductions to Quality Assurance Recording System (QARS) because procurement is complete.
Salary	(2,437)	Reduce overtime and level of awards, specifically funding for merit promotions and regional overtime.
Logistics: Contracts	(2,360)	No anticipated impact due to significant progress made in enhancing logistics capability.
Salary	(1,626)	Institute systemwide salary cap, limiting overtime, awards, etc.
Mitigation: Contracts	(2,524)	While this will not impact operations, this cut will reduce research, assessment, technology, and support contracts.
Grants/cooperative agreements	(826)	Reduce dam safety and earthquake assistance funding.
Salary	(1,624)	Institute systemwide salary cap, limiting overtime, awards, etc.
National continuity programs: Travel	(760)	Reduce general and conference travel.
Contracts	(13,740)	Nonrecur funding for one-time costs for IPAWS and classified program; reduce program support to discussion—based exercises.
Office of the Administrator: Travel	(1,816)	Reduce general and conference travel by leveraging Web conferencing and other technology tools to continue outreach activities and sustain training with State and local partners.
Contracts	(2,046)	Reduce program support contract and professional services, specifically for OCFO by leveraging existing in-house capabilities.
Equipment	(596)	Reduce nonmission-critical equipment purchases.
Salary	(236)	Institute system wide salary cap, limiting overtime, awards, etc.
Mission Support Bureau: Facilities enhancement	(23,300)	Nonrecur one-time increase.
Business systems investment	(5,000)	Reduce investment—operate in maintenance mode.
Contractual in-sourcing	(7,503)	Convert contracts to permanent positions/in-source.
Travel	(1,428)	Reduce general and conference travel by leveraging Web conferencing and other technology tools to continue outreach activities and sustain training with State and local partners.
Contracts	(5,808)	Reduce program office support and contract services by leveraging existing in-house capabilities.

FISCAL YEAR 2012 MANAGEMENT AND ADMINISTRATION REDUCTIONS—Continued

[Dollars in Thousands]

Directorate/office	Fiscal year 2011 to fiscal year 2012 reductions	Impact statement
Equipment	(4,106)	Reduce non mission-critical equipment purchases; institute telecommunications efficiencies.
Office of National Capital Region Coordination:		
Contracts	(1,200)	Nonrecur funding for the completion of knowledge management system (a la Wikipedia) for risk and reduce contracts.
Salary	(302)	Institute system-wide salary cap, limiting overtime, awards, etc.

Note: Annual national level exercises may be funded differently depending upon the exercise. Integrated Public Alert and Warning System (IPAWS) retrofitting would be delayed.

FEMA STAFFING

Question. What method is used to calculate FEMA full time equivalent (FTE) usage? Does it vary from the simple calculation of number of hours worked divided by an FTE? Is there a unique calculation for FTE usage funded from disaster relief?

Answer. FEMA FTE usage is based upon actuals (for fiscal year 2010) and projections (for fiscal year 2011 and 2012) of hours worked divided by the number of hours for one FTE. There is no unique calculation for FTE usage funded from the DRF.

CATEGORIES OF EXPENDITURE FOR GRANT PROGRAMS

Question. For the State Homeland Security Grant Program, the Urban Area Security Initiative, the Port Security Grant Program, and the Public Transportation Security Assistance Program please provide the amount spent in each capability category such as communications, planning, Chemical, Biological, Radiological, Nuclear, Explosive (CBRNE) detection, intelligence and information sharing, and volunteer management and donations for fiscal years 2005–2009.

Answer. The State Homeland Security Program (SHSP), Urban Areas Security Initiative (UASI), Transit Security Grant Program (TSGP), TSGP Supplemental, and TSGP ferry grant funding are comprised of 38 principal capabilities that provided more than \$6.5 billion in funding from fiscal year 2006–2009.

The table below provides the information requested to the extent possible under the Grant Reporting Tool:

SELECT GRANT PROGRAMS TARGET CAPABILITY FUNDING REPORT

Capabilities ¹	Fiscal year 2006–2009 Funding amount
Animal disease emergency support	\$20,743,442.08
CBRNE detection	386,704,474.13
Citizen evacuation and shelter-in-place	31,075,070.88
Communications	1,367,698,117.53
Community preparedness and participation	185,274,333.67
Counter-terror investigation and law enforcement	304,083,757.85
Critical infrastructure protection	1,116,113,358.21
Critical resource logistics and distribution	75,601,714.40
Economic and community recovery	10,568,637.65
Emergency operations center management	191,436,101.57
Emergency public information and warning	41,524,731.18
Emergency public safety and security	248,819,560.09
Emergency triage and pre-hospital treatment	25,344,823.98
Environmental health	1,764,190.73
Epidemiological surveillance and investigation	11,453,350.84
Explosive device response operations	138,614,977.97
Fatality management	13,842,672.26
Fire incident response support	133,775,284.91
Food and agriculture safety and defense	18,742,044.82
Information gathering and recognition of indicators and warnings	68,173,961.12
Intelligence analysis and production	98,482,865.34

SELECT GRANT PROGRAMS TARGET CAPABILITY FUNDING REPORT—Continued

Capabilities ¹	Fiscal year 2006–2009 Funding amount
Intelligence and information sharing and dissemination	282,124,151.92
Isolation and quarantine	3,479,732.45
Laboratory testing	4,893,098.88
Mass care (sheltering, feeding, and related services)	46,925,998.01
Mass prophylaxis	28,444,288.70
Medical supplies management and distribution	25,236,254.98
Medical surge	92,422,098.42
Onsite incident management	169,964,547.36
Planning	898,629,834.82
Responder safety and health	54,272,195.33
Restoration of lifelines	6,585,975.25
Risk management	33,036,019.11
Search and rescue (land-based)	70,162,612.74
Structural damage assessment	1,039,802.34
Volunteer management and donations	4,143,404.68
Weapons of mass destruction and hazardous materials response and decontamination	307,023,005.21
Grand Total	6,518,220,491.41

¹ This table includes FEMA SHSP and UASI.

GRANTS TO STATE AND LOCAL GOVERNMENTS FOR FIRST RESPONDERS

Question. In this Nation we have set up a system whereby, the smallest level of government is responsible for responding to a disaster until it is overwhelmed and then it must work with other communities, States, the private sector, and the Federal Government depending on the size of the disaster. No doubt, State and local first responders will be the first on the scene during an incident. When there is a catastrophic event, the whole Nation will have to respond. Because of this, few disagree that each level of government has to contribute resources to prepare for, respond to, mitigate against, and recover from such events. However, many disagree on how much should be contributed and from what entity. This disagreement has been further highlighted as resources at all levels become more limited. Each year the President's budget is submitted with the same proposal purporting to streamline grant programs. Each time that proposal has been rejected due to a lack of understanding of how it will actually be implemented, its inconsistency with the underlying authorization law, and concerns from stakeholders. Further, the Department has yet to submit a metric to demonstrate how the grants are best targeted to needed capabilities. Since our emergency management environment is continually evolving, the issue of Federal grants to support State and local preparedness is also dynamic. For this reason, the report accompanying the Department of Homeland Security Appropriations Act, 2010 created a preparedness task force which made specific recommendations related to funding grants and measuring their performance. Further, the specific authorized funding levels for many of the grant programs authorized in the 9/11 Act will end in fiscal year 2012. The next step is for the executive branch to provide leadership for an innovative approach to grant programs that can be supported by stakeholders. Yet there is very little evidence that a commitment to this effort is real by FEMA or the Department. Secretary Napolitano, this issue is not only one of citizen safety and security but it is also an economic imperative to make the Nation more resilient through better preparedness and more efficient recovery.

Will the Department propose legislation to reform the grant programs?

What innovative approaches can you introduce which will also be supported by stakeholders, to ensure our State and local partners in homeland security and emergency management are sustaining the right capabilities for our known and anticipated risks?

Who specifically in your agency is responsible to lead the issue of preparedness and Federal grants and what products will you require of them in fiscal year 2011 and fiscal year 2012 to ensure policy and requested funds are meeting the Nation's needs? What timeframe will you hold them to on these products?

Answer. In its last two budgets, the administration has proposed consolidating grant programs where activities are allowable under multiple grants. Specifically, the fiscal year 2011 and 2012 budgets propose to consolidate a number of individual grant programs (including driver's license security/real ID, interoperable emergency

communications, emergency operations centers, and buses) and make them part of larger/broader grant programs such as UASI and SHSP. This consolidation will reduce the number of separate grant programs, which provides the Secretary flexibility to direct funding to the most urgent priorities and reduces the number of applications a State will need to submit and that FEMA will need to process.

FEMA agrees with recommendation #14 in the Local, State, Tribal, and Federal Preparedness Task Force's report to the Congress, which calls for "Threat and Hazard Identification and Risk Assessment (THIRA) processes at all levels of government to establish a foundation to justify preparedness improvements." The detailed recommendation came directly from the stakeholder community.

FEMA's Deputy Administrator for Protection and National Preparedness (PNP), Timothy Manning, is responsible for the Agency's preparedness and Federal grant responsibilities. Within FEMA/PNP, the Grant Programs Directorate (GPD) is responsible for the administration of preparedness grants; and the National Preparedness Directorate (NPD) is responsible for preparedness activities, including individual and community preparedness, planning guidance, technical assistance, training, exercises, preparedness doctrine and policy, and preparedness assessments.

FEMA has taken the recommendations from the Local, State, Tribal, and Federal Preparedness Task Force report into consideration while working to improve coordination and consolidation of FEMA's grant programs, including coordinating inter-agency grant programs and more closely linking capability assessments to grant activities. FEMA has also contracted with the National Association of Public Administration (NAPA) to conduct a study to develop a core set of performance measures that can be used to track performance of the SHSP and UASI grants.

NATIONAL DOMESTIC PREPAREDNESS CONSORTIUM

Question. The President's budget request proposes deep cuts, 56 percent, to first responder training through the National Domestic Preparedness Consortium (NDPC). It proposes to cut funding for four members of the NDPC who train emergency personnel from all over the country to respond to weapons of mass destruction, including chemical, biological, radiological, nuclear, and explosives attacks. Further, it completely eliminates funding for two members: one that provides training for response to natural disasters and one that provides training specific to transit related incidents. I do not understand these cuts, especially when the NDPC uses a cost-effective model that sends instructors to the community receiving training when possible reducing the travel, accommodations, and backfill expenses of first responders. What is the Department's justification for cutting funding to this highly regarded training for first responders? Further, in light of the fact that the United States was struck by more than 106 natural disasters last year and there have been more than 1,300 attacks, killing or injuring more than 18,000 people worldwide on trains and subways over the last 7 years worldwide why is training funding eliminated for natural disaster response training and transit response training when these are clearly known risks?

Answer. The fiscal year 2012 President's budget is consistent with the fiscal year 2010 and fiscal year 2011 proposals, and the resources requested are sufficient to meet training needs. The two recipients whose funding was eliminated represent congressional earmarks. In addition, States are assuming increased responsibility for awareness level, refresher, and sustainment training, allowing our institutional partners to focus resources on more advanced, specialized training consistent with their respective expertise. Further, States are permitted to support hazard-specific training efforts with SHSP and UASI grant programs funds, both subject to proposed fiscal year 2012 increases overall.

URBAN AREA SECURITY INITIATIVE

Question. The House fiscal year 2011 continuing resolution includes a provision that limits the number of UASI grant recipients to 25. Some argue that the list should be even shorter and only support the cities in the top tier of risk. The 9/11 Act requires the FEMA Administrator to complete an annual risk assessment of the 100 most populous urban areas and to determine grant awards based on that risk review. Last year 64 urban areas received funding based on your risk assessment.

What specifically led you to determine that risk is more widespread than some others believe? What is your position on the House amendment to reduce the number of urban areas from 64 to 25? How will the House amendment impact how risk is addressed in the Nation?

Answer. Historically, al Qaeda has focused on prominent political, economic, and infrastructure targets to produce mass casualties, visually dramatic destruction, sig-

nificant economic aftershocks, and fear among the population. The UASI program was authorized and implemented to reduce the vulnerabilities of our key metropolitan areas to these types of terrorist threats. While mostly outside the scope of the UASI program, recent events suggest a trend in which terrorists seek to conduct smaller, more achievable attacks against easily accessible targets. Within the past year, attempted attacks and plots in the United States progressed to an advanced stage largely because of these groups' ability to use operatives that have access to and familiarity with the United States as well as their use of new and varied attack patterns.

DHS and FEMA leadership have awarded grants to UASI-eligible cities using an allocation methodology that was a continuation of prior approaches to awarding these types of grants. To determine the UASI-eligible cities, DHS and FEMA apply a risk formula that incorporates threat, vulnerability, and consequence. The administration is committed to working with the Congress, as it seeks to improve upon current risk-informed approaches.

The fiscal year 2011 Homeland Security full-year appropriations bill did not limit the number of eligible UASI cities to 25. As directed in section 101 of the 9/11 Act, which amends title XX, sections 2003 and 2007 of the Homeland Security Act, FEMA will continue to assess on an annual basis the relative risk of the 100 most populous metropolitan statistical areas.

EMERGENCY FOOD AND SHELTER PROGRAM

Question. I understand the Emergency Food and Shelter Program uses a very specific formula to distribute funding based on unemployment data and poverty figures. While there are signs that the economy is improving, the recovery has not yet reached those who are the hurting the most the unemployed and the poor. What economic data was used as the basis for the proposed reduction to \$100 million?

Answer. The fiscal year 2012 President's budget for the Emergency Food and Shelter (EFS) Program at the \$100 million level is consistent with the level requested in the President's budget for fiscal year 2010 and fiscal year 2011.

FEMA awards the total funds appropriated by the Congress to the National Board for the EFS Program, as required by the McKinney-Vento Homeless Assistance Act. The National Board then allocates the funding to approximately 2,500 local jurisdictions in all States and territories using a formula based on the latest 12-month statistical data on national unemployment and poverty provided by the U.S. Bureau of Labor Statistics.

NATIONAL FLOOD INSURANCE PROGRAM AND FLOOD MAPS

Question. Annual flood losses in the United States total more than \$2.4 billion. More than 5.5 million people currently hold flood insurance policies in more than 20,500 communities across the United States.

The Nation's flood maps, managed by FEMA, help us assess the risk a community faces and determine how to insure against that risk. Unfortunately, the process used to develop these maps is cumbersome and lacks an ability to apply common sense solutions to a community's unique factors. I understand that we have to insure against floods, but in this day and time, it also has to be affordable.

Recognizing that the Congress, through the Banking Committee which has jurisdiction over this matter, is considering significant reform to the National Flood Insurance Program, FEMA began a critical review of the program. The review is projected to be completed as late as June of 2012. I just don't think people can wait that long for reform. The National Committee on Levee Safety, which was established by the Congress and includes representatives from FEMA and the Corps of Engineers, issued recommendations for reforms back in January 2009. Some have called for stopping the mapping process altogether and others want to move forward but include measures that improve local capacity and map accuracy. Twenty-seven Senators, including myself, and 49 House Members, wrote to you last month to express concerns about the program and to propose specific reforms.

Are you satisfied that the Nation is moving as quickly as possible on this matter? What can be done to expedite the executive branch's proposal for reform?

Answer. Currently, FEMA is executing the National Flood Insurance Program (NFIP) Reform work plan, and is evaluating changes to the program. This process was designed to engage program stakeholders from a variety of perspectives, and to date has included hundreds of stakeholders in a series of public meetings and generated thousands of public comments on reform possibilities.

The original NFIP reform work plan envisioned an 18-month process, to ensure thorough and transparent engagement with a wide variety of program stakeholders. Based on feedback from the Congress, FEMA has accelerated this schedule, and

hopes to report findings before the end of this 18 months timeframe. This will allow for consideration of program reforms by decisionmakers prior to the expiration of the current NFIP authorization in September 2011.

FLOOD HAZARD MAP RISK ANALYSIS (FHMRA) AND MODERNIZATION

Question. To date, \$1.65 billion has been provided to digitize flood maps, and in many cases, improve the data used to create maps. How many maps, by State, still need to have significantly improved engineering data/validated data added to the maps? Please provide a comparison of the number of maps that will be produced if the budget request of \$103 million is provided for FHMRA compared to the fiscal year 2010 level.

Answer. FEMA tracks the flood hazard inventory by stream and coastal miles. Our total modernized inventory is comprised of about 900,000 miles. The national need stands at 59 percent of stream miles (currently 41-percent valid). This means about 530,000 miles of the inventory needs updating to reach 100 percent valid. The goal in the Risk MAP multi-year plan was to reach 80 percent valid. This equates to 350,000 miles. As a percentage of the modernized map inventory of about 100,000 maps, about 59,000 maps need updating to reach 100 percent, 39,000 maps need updating to reach 80 percent valid.

At the fiscal year 2010 funding level, FEMA would begin updating 9,000–12,000 maps. Under the proposed funding level for fiscal year 2012, FEMA estimates 6,000 to 8,400 maps less per year will be produced. FEMA will adapt its project sequencing process in an aim to keep pace with the eroding reliability of the flood hazard analyses and maps.

The data presented below is from a data collection done on January 28, 2011, and shows the percentage of miles by State that are currently invalid. This information is improving regularly. The national need stands at 59 percent of stream miles (currently 41-percent valid).

FEMA NATIONAL FLOOD HAZARD INVENTORY

[Percentage of stream and coastal miles by State currently needing updates]

State	Percentage of miles needing significantly improved engineering data/validated data
Alabama	42
Alaska	1
Arizona	99
Arkansas	69
California	93
Colorado	70
Connecticut	98
District of Columbia	12
Delaware	58
Florida	88
Georgia	39
Hawaii	99
Idaho	99
Illinois	93
Indiana	85
Iowa	13
Kansas	30
Kentucky	14
Louisiana	86
Maine	99
Maryland	37
Massachusetts	98
Michigan	30
Minnesota	37
Mississippi	51
Missouri	47
Montana	81
Nebraska	10
Nevada	92
New Hampshire	96

FEMA NATIONAL FLOOD HAZARD INVENTORY—Continued
[Percentage of stream and coastal miles by State currently needing updates]

State	Percentage of miles needing significantly improved engineering data/validated data
New Jersey	73
New Mexico	43
New York	38
North Carolina	57
North Dakota	72
Ohio	39
Oklahoma	60
Oregon	95
Pennsylvania	38
Rhode Island	98
South Carolina	37
South Dakota	92
Tennessee	23
Texas	83
Utah	94
Vermont	94
Virginia	79
Washington	95
West Virginia	75
Wisconsin	83
Wyoming	99

¹ Not yet available.

UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES—INTERNATIONAL
ADOPTIONS—HAITI

Question. The Help HAITI Act, which was enacted in December 2010, responded to the need for the families of the 1,400 Haitian orphans who were granted humanitarian parole in the aftermath of the January, 2010, earthquake, to immediately apply to adjust the immigration status from parolee to legal permanent resident. Prior to the enactment of the Help HAITI Act, these orphans, upon finalizing their adoptions by American families in U.S. State courts, would have had to wait for 2 or more years to adjust their immigration status to legal permanent resident. During this 2-year period, these vulnerable children would have remained in limbo, leaving them with fewer legal protections, potentially ineligible for critical resources, and at risk of being returned to Haiti.

Several Members, including myself, sent you a letter asking for the swift implementation of the Help HAITI law, to ensure that families are able to move towards naturalization as soon as possible. You responded to our letter on February 7, 2011, and noted that many of the suggestions we had made to streamline the process for the adoptive families have already been implemented by the Department. I appreciate what has been done to date in this regard.

Can you please identify the specific steps you have taken towards the implementation of the Help HAITI Act? Are there additional steps that the Congress needs to take legislatively to assist these families with these adoptions?

As you know, I am deeply concerned about how the Congress can work with your Department—and other Departments involved in the international adoption process—to safely and efficiently improve this process so that adoptive parents can be joined with children eligible for adoption. I hope you will commit to working with me on this issue.

Answer. The following is a timeline of steps U.S. Citizenship and Immigration Services (USCIS) took to implement this law:

- Sent a letter to each of the parents/sponsors of paroled Haitian children to advise them of the passage of the act. The letter also informed them that additional information would be sent to them and that the USCIS Web site would be updated with information about filing under the act. (12/16/2010)
- Implemented an interim policy for implementation of the act. (12/21/2010)
- USCIS Web site announcement posted about the act's implementation. (1/3/2011)

- Filing instructions posted on the USCIS Web site. (1/4/2011)
- A follow-up letter was sent out to the parents/sponsors of paroled Haitian children with instructions on how to apply under the act. (1/5/2011)
- Teleconference held for families of paroled Haitian children and other external stakeholders. (2/9/2011)
- USCIS systems updated to produce the Green Cards reflecting the newly established class of admission code HH-6. (2/27/2011)

Through March 14, 2011, approximately 30 individuals had filed applications to adjust status under the act. The act established a cap of 1,400 through December 9, 2013. USCIS is closely monitoring the number of applicants and approvals. USCIS will contact at a later date the parents/sponsors of the children that have not yet filed to remind them of the act.

As the provisions of the act will permit all children authorized parole under the Special Humanitarian Parole Program to obtain lawful permanent status in the United States, the Department does not believe additional steps or legislation is needed.

INTERNATIONAL ADOPTIONS—CAMBODIA AND NEPAL

Question. USCIS has played a central role in the processing of orphan visas for the nearly approximately 200,000 children adopted by United States citizens over the last decade. I know that this role is not one that is taken lightly and appreciate the work that you and your Department have done to make the adoption of children from other countries both efficient and ethical. That being said, I remain concerned that USCIS has felt there was no alternative in at least two countries, almost 10 years ago in Cambodia and most recently in Nepal, than to suspend orphan visa processing altogether. To me, suspending adoptions in response to allegations of fraud is like shutting down the international banking system because of a bank robbery. We need to find a better more targeted way of using the law to preventing abuse and then actively prosecuting those who abuse the law.

Please provide the subcommittee with examples of ways we might work together to provide the Department with alternative measures to protect children, their birth families, and their potential adoptive families?

Answer. The Department believes that the best way to respond to concerns about abuse in the intercountry adoption context is through implementing better safeguards and protections in the process. I share your concerns about the total suspension adoption processing in certain countries. Where possible, the better approach is to identify and seek to address specific problems in adoption programs without suspending them completely. The Hague Adoption Convention, which entered into force for the United States in 2008, implements procedures for intercountry adoption processing that include many important safeguards helping guarantee the transparency and integrity of the adoptions process.

The Department supports a U.S. Government approach of working proactively with countries of origin that have not yet signed or ratified the Hague Adoption Convention to assist them in developing the appropriate child welfare infrastructure needed for Hague implementation. In the meantime, DHS also supports making changes to U.S. non-Hague adoption immigration processing policy and procedures that include some of the protections of Hague policy and processing, particularly those that enhance transparency and integrity in intercountry adoption.

In August 2010, the Department of State (DOS) identified a serious concern in the processing of adoption cases from Nepal involving children presented as abandoned—namely that the documentation provided by the Nepali police validating the abandonments of the children was unreliable and not credible. DOS and USCIS conducted a joint investigation which resulted in the suspension of processing of new abandonment cases for Nepali children. Since then, DOS and USCIS have been processing the 64 abandonment cases that were already in progress as of the suspension date, all but 6 of which have required detailed Requests for Additional Evidence because the initial documentation provided with the adoption petitions failed to establish that the children could be defined as orphans under U.S. law. This suspension affected only abandonment cases in Nepal, and the program remains open for cases involving relinquished children. The processing of the 64 abandonment cases is ongoing.

The Department will continue to look for ways to strengthen international adoption policies and operational practices to the benefit of children and families, and looks forward to working closely with the Subcommittee on this issue.

Question. What activities did funds provided to E-Verify for Monitoring and Compliance support in fiscal year 2010? What metrics are in place to track the success of the Monitoring and Compliance division in ensuring employer compliance with system rules?

What steps can a worker currently take to challenge an erroneous final nonconfirmation? Are there any forms of redress, reconsideration, or protections in place for workers who lose their job as a result of an erroneous final nonconfirmation? What is the estimated cost of making E-Verify mandatory nationally?

A recent Government Accountability Office report called USCIS's prior cost estimate "minimally credible". What steps are being taken to further improve the accuracy of cost assessments? What fiscal impact would making E-Verify mandatory have on small businesses?

Bloomberg Government reported that if E-Verify had been mandatory for all employers in 2010, it would have cost businesses \$2.7 billion–\$2.6 billion of which would have been borne by the small businesses that drive our economy. Does USCIS concur in that estimate? If not, please explain why?

Answer. In fiscal year 2010, the E-Verify Monitoring and Compliance (M&C) program continued to expand in terms of capacity, compliance and initiatives to enhance the integrity of the E-Verify system. Hiring and recruitment were underway for an additional 44 M&C staff. As of the beginning of March 2011, 13 were on board and 20 are in clearance. To increase M&C staff's capacity to process more cases, an enhancement was made to the Compliance Tracking and Management System, which helped to streamline processing and decrease manual data entry. System requirements for an enhanced data analytics tool were completed in fiscal year 2010 in anticipation of fiscal year 2011 procurement, allowing more detailed and full analysis of employer behavior. In terms of compliance activities, M&C contacted approximately 15,000 employers related to noncompliance.

M&C also started tracking additional employer actions. These actions include monitoring for:

- Duplicate Social Security numbers (two reports);
- Verifying employees hired before November 7, 1986 (employers must complete the Form I-9 before using E-Verify, and employers may not use the Form I-9 for employees hired before November 7, 1986);
- Nonuse of E-Verify;
- Terminating employees following a Tentative Nonconfirmation (TNC);
- Verifying an employee more than 3 days after he or she was hired; and
- Verifying existing employees.

M&C also executed a Memorandum of Understanding related to sharing of information and monitoring employer actions referred to it by the Department of Justice Civil Rights Division's Office of Special Counsel for Immigration-Related Unfair Employment Practices.

More than 45,000 employers who have signed new agreements with E-Verify have been vetted through Dun & Bradstreet to ensure that companies enrolling in E-Verify are legal and active corporate entities. This further strengthens the integrity of the system by verifying the legitimacy of employers using the system. USCIS plans to ensure all of the 250,000 employers are vetted in the coming year.

E-Verify system enhancements have also included new closure codes to be used by employers to ensure resources are devoted to cases that may point to possible misuse of the system. For example, this change helps M&C analysts have more insight as to whether an employee run through E-Verify was terminated as a result of an E-Verify finding or if they quit voluntarily.

An important enhancement to E-Verify was the addition of passport data and photos as part of our continuing efforts to address identity fraud and employee use of falsified documents.

Regarding metrics, M&C monitors employers who were subject to compliance action. Fiscal year 2010 data indicate that 90 percent of employers corrected past processes and are now in compliance with E-Verify program rules and policies for which they received compliance assistance.

USCIS is committed to ensuring that workers who receive a final nonconfirmation in error are treated equitably. Even if an employee receives a final nonconfirmation, the employer may retain the employee provided that it notifies DHS. Section c.6 of the E-Verify Memorandum of Understanding signed by the employer states, "The employer must notify DHS if it continues to employ any employee after receiving a final nonconfirmation, and is subject to a civil penalty between \$550 and \$1,100 for each failure to notify DHS of continued employment following a final noncon-

firmation.” The employer may notify DHS by selecting the following option when closing out the case in the E-Verify system:

—The employee continues to work for the employer after receiving a final nonconfirmation result. E-Verify cannot verify that this employee is authorized to work in the United States. The employee had contested the tentative nonconfirmation, but was unable to resolve it. The employer chooses to exercise its legal right to allow the employee to continue to work.

Employees who believe that they received a final nonconfirmation in error have called either the E-Verify employee hotline or the Office of Special Counsel (OSC) for Unfair Immigration-Related Employment Practices. USCIS and OSC have a coordinated process for intervening on the employees’ behalf. Both telephone numbers are found on employee tentative nonconfirmation notices and referral letters.

E-Verify staff will assist the small number of employees who receive a final nonconfirmation in error and intervene on their behalf. Specifically, USCIS and OSC have helped employees return to their jobs after they were terminated for receiving a final nonconfirmation by contacting their employers and explaining to them that the final nonconfirmation was issued in error. In a minority of overturned final nonconfirmation cases, OSC was also able to get back pay for employees in addition to getting them reinstated.

To help employees avoid the adverse consequences associated with erroneous final nonconfirmations, USCIS will begin a phased deployment of Self Check in March, 2011. Self Check provides individuals with the ability to confirm their own employment eligibility status. For those individuals who will be working for an E-Verify employer, Self Check will enable them to identify any potential data mismatches before employment begins and the employer runs an E-Verify check. E-Verify Self Check is not for employer use. Employers may not require workers to use Self Check or show Self Check results.

The estimated cost of making E-Verify mandatory would depend on the details of legislation making the system mandatory, fully considering all relevant factors and cost drivers.

The recent GAO findings were based solely on cost estimates related to the Verification Information System’s (VIS—the IT system that supports E-Verify) Life Cycle Cost Estimates (LCCE). Significant revisions have been made since the review by GAO. In addition to performing sensitivity and risk analyses of the data, an independent reviewer (i.e., the MITRE Corporation) analyzed the revisions to determine whether the new estimates possessed the four characteristics identified by GAO as being reliable cost estimates:

—*Comprehensive*.—According to MITRE’s analysis, the current version of the estimate now breaks each enhancement project into smaller elements using the phases of the Systems Engineering Life Cycle (SELC) as a model. The estimate now incorporates historical cost data, but still does not include some external program costs for activities such as Operation and Maintenance (O&M) and security costs which are funded by the USCIS Office of Information Technology (OIT). There is ongoing effort related to this evaluation to include these costs.

—*Well Documented*.—Methods used to develop the estimate are now clearly documented and presented in a manner as to be recreated by someone unfamiliar with the estimate. The current version of the estimate now contains an accompanying workbook detailing the data and calculations used in deriving all estimates and a risk register was created that identifies specific program risks.

—*Accurate*.—The current LCCE has been updated to reflect programmatic changes as of the second quarter of fiscal year 2011, including actual Social Security Administration (SSA) cost projections.

—*Credible*.—The estimate now contains both sensitivity and risk analysis sections consistent with best practices outlined by GAO. The MITRE review also found that an underestimation of the cost risk. This issue has been addressed and a more realistic method of correlation estimation has been used.

Regarding the fiscal impact on small businesses of making E-Verify mandatory, at this time, USCIS does not have data and analysis that would specify the potential impact. USCIS will consider conducting analysis on this matter in the future.

FEDERAL LAW ENFORCEMENT TRAINING CENTER (FLETC)

Question. At the February 17, 2011 Homeland Security and Governmental Affairs hearing, the Secretary said FLETC recently piloted a test curriculum on homegrown violent extremism with participation from local police and sheriff departments. Please provide more information about this pilot program. How will this change or expand FLETC’s current missions and curricula focus? What is the plan to continue

pilot testing, rolling out the program? Who will the training focus on? State and local? Rural, urban, Federal law enforcement?

Answer. In February 2010, I tasked the Homeland Security Advisory Council (HSAC) to work with State and local law enforcement as well as relevant community groups to develop recommendations on how the Department can better support community-based efforts to combat violent extremism domestically. To this end, HSAC established a Countering Violent Extremism (CVE) working group consisting of law enforcement, community leaders, State and local government officials, youth leaders, academic leaders, and other subject matter experts to provide a series of recommendations.

In response to these recommendations, DHS has been working with Federal partners as well as State and local law enforcement organizations to develop guidance for the development of CVE training.

A proof of concept session, based on the newly drafted curriculum guidance, was hosted at FLETC in Glynnco, Georgia from February 8–10 and included State, local, and tribal law enforcement officials from around the country. Participants received preexisting FLETC CVE related training, after which they discussed the training and provided feedback. A training needs assessment was conducted during the session to identify the appropriate scope and direction of the CVE training. Findings were compared against nationally recognized and emergent best practices for similar topics. The participants identified four crucial topical areas:

- Community-oriented policing;
- Cultural awareness;
- Information sharing, including suspicious activity reporting and intelligence-related information processes; and
- Civil rights and privacy.

In addition, the participants identified the need for at least two versions of the CVE training: an executive level course, targeting command level law enforcement leadership; and a line officers course, targeting patrol officers and investigators.

As a result of the curriculum development session, the FLETC will develop the Countering Violent Extremism Training Program (CVETP), in collaboration with State and local police stakeholders and subject matter experts. The training will focus on State, local, and tribal law enforcement officers who serve in urban and/or rural environments. In addition, CVE training will be incorporated into existing training programs for Federal officers and agents conducted at the FLETC.

Next steps in rolling out the program include the Design Phase, which involves a Curriculum Development Conference (CDC) to finalize training topics, write performance objectives and outline the training schedule; the Development Phase, which will encompass resource identification, lesson plan and training materials development, and determination of instructional methodologies; and the pilot program, which will test the validity of the established CVETP goals and objectives. Delivery of the pilot program is expected within 120 days following the CDC.

Following delivery of the pilot program, the CVETP will begin the Evaluation Phase to determine program content and criterion validity. Participant feedback will be collected, instructors will be evaluated, and any adjustments to the curriculum identified as a result of the delivery of the pilot will be incorporated into the CVETP prior to full implementation. Using a combination of delivery mechanisms, 400–600 students are expected to be trained during fiscal year 2011 and 2,400–3,600 in fiscal year 2012. By fiscal year 2013, instructor-led content will be converted to a digital format to allow interactive delivery using an electronic learning portal. As a result, an unlimited number of law enforcement students can potentially be trained using available technologies.

SCIENCE AND TECHNOLOGY—LABORATORY FACILITIES

Question. Provide the distribution of the \$276.5 million request for laboratory facilities, by facility and purpose.

Answer. The table below provides the distribution of the \$276.5 million request for laboratory facilities, by facility and purpose.

	Fiscal year 2012 President's budget request
Construction:	
Infrastructure upgrades ¹	\$18.2
National Bio and Agro-Defense Facility (NBAF)	150.0

	Fiscal year 2012 President's budget request
Operations:	
Chemical Security Analysis Center (CSAC)	0.8
National Urban Security Technology Laboratory (NUSTL)	2.3
Plum Island Animal Disease Center (PIADC)	40.8
Transportation Security Laboratory (TSL)	13.4
National Biodefense and Analysis and Countermeasures Center (NBACC)	30.9
Laboratory salaries and benefits	20.1
Total	276.5

¹ In fiscal year 2012, S&T plans infrastructure upgrades at TSL.

AVIATION SECURITY RESEARCH—AUTOMATED TARGET RECOGNITION

Question. Provide an assessment by the Science and Technology Directorate of the Automated Target Resolution (ATR) technology that is being tested as a software upgrade to Advanced Imaging Technology units? Based on S&T's assessment of this technology, will it be ready for deployment in fiscal year 2011? What is the schedule for certification?

Answer. The Science and Technology Directorate's (S&T) Automated Target Recognition (ATR) project develops advanced software capabilities for AIT units to detect explosives and concealed weapons. This project also will introduce new stand-alone or adjunct imaging technologies, such as computed tomography, to continue the improvement of detection performance and the detection of novel explosives. This is critical to improve detection, lower false alarm rates, and reduce privacy concerns. S&T is currently evaluating advanced threat recognition software to guide further enhancements to reach full-scale development and deployment.

One millimeter-wave based ATR system recently completed qualification testing at the DHS Transportation Security Laboratory. Based on these results, the TSA granted authority to pilot the system for passenger screening purposes at three aviation checkpoint test sites (Hartsfield-Jackson Atlanta International Airport, Ronald Reagan Washington National Airport, and Las Vegas-McCarran International Airport). S&T has approved the system's test and evaluation master plan addendum and the operational test plan. TSA has concluded operational testing and evaluation and the results are currently being compiled and reviewed. The final operational test report is scheduled for May 2011. Once all reports are received, S&T will complete a letter of assessment for the testing.

DOMESTIC NUCLEAR DETECTION OFFICE—RADIATION PORTAL MONITOR (RPM) PROGRAM

Question. Provide a status update of RPM requirements by vector including total RPMs required by vector, systems deployed, and the percentage completed. Indicate gaps where solutions do not exist. The request includes \$37.4 million for RPM acquisitions. How will this money, in addition to unobligated balances, reduce the gap in RPMs necessary at each vector? Provide a plan for RPM unobligated balances and the \$37.4 million requested for fiscal year 2012. Distinguish between current generation and ASP deployments. How is the Helium-3 shortage impacting this program? Has a solution been identified?

Answer. The response to this question is designated as For Official Use Only (FOUO). The Department will submit the response under separate cover.

HUMAN PORTABLE RADIATION DETECTION SYSTEMS

Question. For Human Portable Radiation Detection Systems (HPRDS), provide a chart showing the notional fiscal year 2012 acquisition plan by technology, the quantity, and by DHS component. What is the total number of HPRDS needed by each component?

Answer. The chart below provides the notional fiscal year 2012 acquisition plan by technology, the quantity, and by DHS component.

Fiscal year 2012	Cost	Quantity	Total (in millions of dollars)
CBP:			
(LaBr) next generation handhelds	\$30,000	340	10.0

Fiscal year 2012	Cost	Quantity	Total (in millions of dollars)
(HPGe) next generation advanced handheld (upgrade)	100,000	2	0.20
USCG:			
(LaBr) next generation handhelds	30,000	100	3.00
Personal radiation detectors	2,800	700	1.94
DNDO:			
TSA-VIPR Procurement ¹ :			
Recapitalization			1.00
MDDP Procurement:			
Radio-Isotope Identification Devices (RIID) handhelds	23,000	51	1.17
Personal radiation detectors	2,800	72	0.20
Backpacks	34,000	33	1.12
Communication equipment			0.37
³ He Procurement			1.00
Total			20.00

¹ Equipment replacement is due to damage. If substantive damage does not occur, new next gen handhelds will be procured.

Based on present requests, the following is the estimated number of HPRDS needed by component and type of equipment for fiscal year 2011–2017:

	Fiscal year 2011–2017
CBP:	
Next generation advanced handhelds	20
Next generation advanced handheld (upgrades)	2
Next generation handhelds	3,200
Personal radiation detectors	4,400
HPT ¹	150
TSA:	
Backpacks	80
Next generation handhelds	160
Personal radiation detectors	300
HPT ¹	150
USCG:	
Next generation advanced handheld (upgrades)	8
Next generation handhelds	1,000
Personal radiation detectors	4,000
Backpacks	250
HPT ¹	1,600
DNDO (MDDP): Upgrade equipment (# of teams)	3

¹ Note: Human Portable Tripwire (HPT).—The current-generation of human portable systems is predominantly composed of Personal Radiation Detectors (PRDs). The tripwire role is intended to increase the opportunity and likelihood of detecting rad/nuc material through constant, nondeliberate rad/nuc scans. HPT detection systems used to perform passive monitoring should be considered standard operational equipment capable of being worn by operators at all times. These systems should also be easy to use and cost-effective so they can be easily deployed to a large number of operators, increasing the opportunity for detection. These units will likely occur between fiscal year 2011–2017, subsequent to the completion of HPT development efforts.

SMALL BOAT STAND-OFF DETECTION SYSTEM/ON-DOCK RAIL PROGRAM

Question. According to the request, DNDO will complete an Alternatives of Analysis (AoA) for the Small Boat Stand-Off Detection system and the On-Dock Rail program in fiscal year 2011. When will the AoA be completed? If completed, provide a summary of the AoA findings.

Answer. The Small Vessel Stand-Off Detection (SVSD) Alternative Analysis (AA) is scheduled for completion in December 2011. Due to funding delays associated with the continuing resolutions for fiscal year 2011, this project was delayed by 3 months.

As described in DNDO's CJ, the On-Dock Rail (ODR) Alternatives Analysis (AA) is planned for completion in fiscal year 2012 and is currently scheduled to be completed on March 2012.

RADIATION DETECTION STRADDLE CARRIER

Question. According to the request, DNDO will complete an Operational Assessment of a Radiation Detection Straddle Carrier at the Port of Tacoma, Washington in fiscal year 2011. Has this assessment been completed? What did DNDO conclude from this assessment?

Answer. DNDO is poised to begin this assessment immediately, pending settlement of final support details with operational users. Once begun, the assessment will last about 6 weeks. DNDO will provide the results of this assessment when completed.

RADIATION DETECTION FOR AIR CARGO AND CHECKED BAGGAGE

Question. Describe the work DNDO is conducting with TSA or on behalf of TSA to detect illicit nuclear material in air cargo and baggage.

Answer. In close collaboration with the DHS Science and Technology (S&T) Directorate's Transportation Security Laboratory, DNDO is evaluating whether Computed Tomography (CT) x ray systems, currently deployed throughout aviation pathways to detect explosives, can also be used to detect rad/nuc materials in baggage and small cargo. The program will begin with a baseline system evaluation to determine the basic technical feasibility of supporting our rad/nuc mission. The initial tests, currently underway, will focus on determining if the existing, certified CT systems may be able to be leveraged to also detect rad/nuc materials and test objects of interest. Following analysis of test data and determination of feasibility, DNDO, S&T, and Transportation Security Administration (TSA) will discuss options for potential next steps.

RESEARCH AND DEVELOPMENT PROJECT SUMMARIES

Question. For each individual project funded under DNDO's Research, Development, and Operations appropriation, submit quad charts that include a project description, the technology readiness level, planned demos and deliverables, and a timeline for transition.

Answer. Research and development project summaries follow.

DNDO—SYSTEMS ENGINEERING PROGRAM

Program Description/Objectives

Program Description.—This program provides assistance to maintain the high quality and consistency of the application of systems engineering principles across the multiple DNDO programs, and in implementing both the DHS acquisition directive 102-1 and DNDO's solutions development process. This includes program management, financial administration, customer service and quality assurance tasks, as well as an on-site liaison to facilitate customer service and coordination for the Systems Engineering Support Program contract.

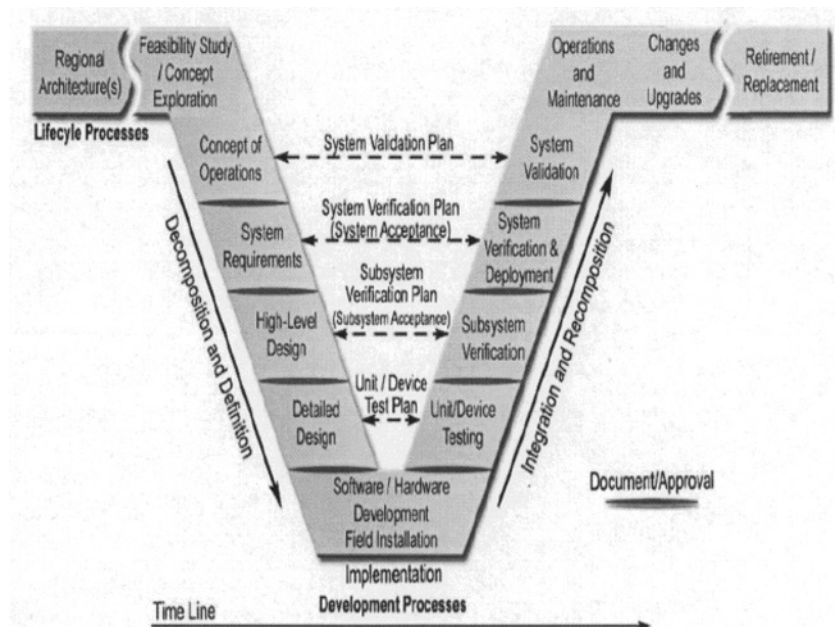
Objectives:

- Institutionalize a systems engineering mindset across DNDO programs and mission areas.
- Assist DNDO program managers and mission area managers in compliance with systems engineering requirements found in DHS Acquisition Directive 102-01.
- Provide engineering support for Aviation Ports of Entry (APOEs).

Fiscal Year 2012 Planned Accomplishments/Milestones

Key Deliverables:

- Leadership and administration will satisfy the commitments of the systems engineering support contract.
- Development of alternatives analysis and operational requirements document for limited deployment of existing technologies to APOEs.
- Conduct analysis of alternatives, characterization testing, and modeling and simulation activities for development of systems for other APOE operational environments.



RD&O—Systems Engineering and Architecture PPA.—Systems engineering program, \$5,400,000.

Technology Readiness Level.—N/A—Not a systems development effort.

Timeline for Transition.—N/A—Not a systems development effort.

GND Alignment:

—GND performance goals 2.1, 2.2, 3.1, 3.2, 4.1, 4.2, 5.1, 5.2, 5.3, and 9.3.

—This task supports all GND detection development and deployment goals.

DNDO—RAD/NUC DETECTION STANDARDS

Program Description

Program Description.—Support for the development and maintenance of domestic and international consensus standards as well as Government-unique standards for radiological and nuclear (rad/nuc) detection systems. DNDO was directed by the Safe Port Act of 2006 to collaborate with NIST and develop Technical Capability Standards (TCS) for nonintrusive imaging and radiation detection equipment to be published by the Secretary of Homeland Security as Government-unique standards. TCS focus on the capability to detect special nuclear material. DNDO and NIST lead an inter-agency standards working group that aims to produce a suite of TCS for various detection systems.

Objectives:

- Aid U.S. Government leadership in the development of national and international standards relating to rad/nuc detection.
- Develop Government-unique TCS for nonintrusive imaging and rad/nuc detection systems.
- Develop and maintain national consensus standards for rad/nuc detection systems.

Fiscal Year 2012 Planned Accomplishments / Milestones

Key Deliverables.—Guidance on required rad/nuc detection capability for users and development programs. Informed by classified threat information not available to entire consensus standard community.

Schedule Goals:

- Develop and revise rad/nuc consensus standards as appropriate.
- Draft two technical capability standards annually until all required standards are published (estimate approximately 12 needed).
- Goal is to complete each TCS in 2 years.

Program Description.—The DNDO Information Sharing Program establishes and maintains the necessary enterprise and data architectures that enable programs in DNDO, DHS, and our Federal, State, local, and commercial partners to effectively share rad/nuc information for the purpose of preventing terrorism and enhancing National Security. Mission Critical Messaging (MCM) will connect Federal, State, local, and tribal radiological and nuclear detection systems to share information for

the purpose of increasing the effectiveness of counter terrorism capabilities and facilitate the development of a rad/nuc information sharing environment. MCM will leverage existing information sharing standards, commercially available technology, and DNDO's JACCIS to connect elements of the GNDA together to share situational awareness and enable a managed coordinated response.

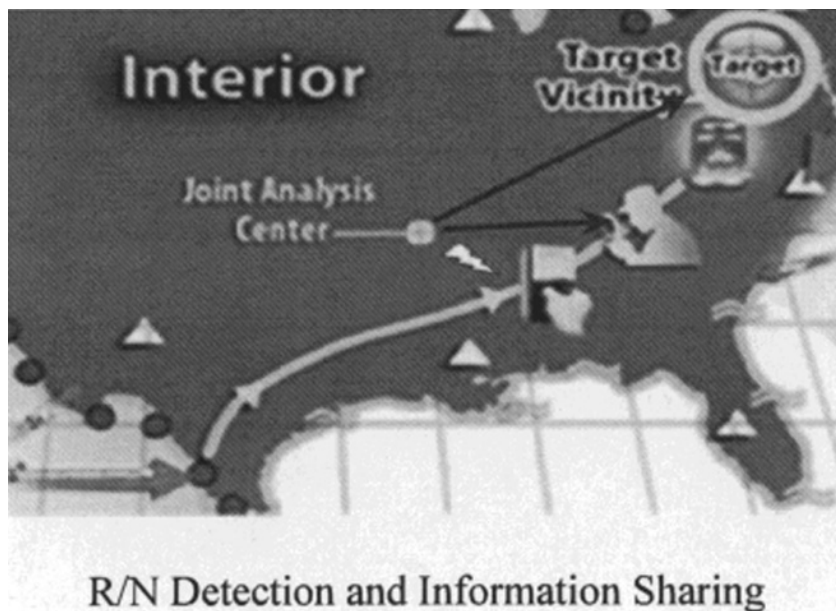
Fiscal Year 2012 Planned Accomplishments/Milestones

Key Deliverables:

- Create and update cost-effective, compliant enterprise architecture, data management, and systems engineering artifacts.
- Update and maintain the National Information Exchange Model (NIEM) chemical, biological, radiological, and nuclear domain, in conjunction with the domain co-steward.
- Update and maintain Information Exchange Package Documentation (IEPD) N.25 standard for rad/nuc information exchange.
- Stand-up the Mission Critical Messaging Project: Plan, analyze, and develop the project approach.
- Establish a test interface between the DNDO Joint Analysis Center (JAC) and at least one Federal, State, local or tribal entity.

Objectives:

- Provide architecture guidance and support to the DNDO programs that support GNDA definition and implementation.
- Improve rad/nuc threat situational awareness among Federal, State, local, and tribal partners.
- Enhance system interoperability to enable faster mission-critical integration.



RD&O—Systems Engineering and Architecture PPA.—Information sharing, MCM, \$5,160,000.

Technology Readiness Level.—TRL will be assessed as part of SDP stage 2a.

Timeline for Transition.—Stage 2a scheduled for fiscal year 2012.

GNDA Alignment.—GNDA performance goals 4.2, 5.2, 6.3, 7.1, and 7.2.

DNDO—GNDA DEVELOPMENT: ANNUAL PLANNING, MODELING, AND ANALYSIS

Program Description/Objectives

Program Description.—Strategic planning and evolving risk evaluations contribute to an a Joint Inter-agency Annual Review and Annual Report on the GNDA that provides:

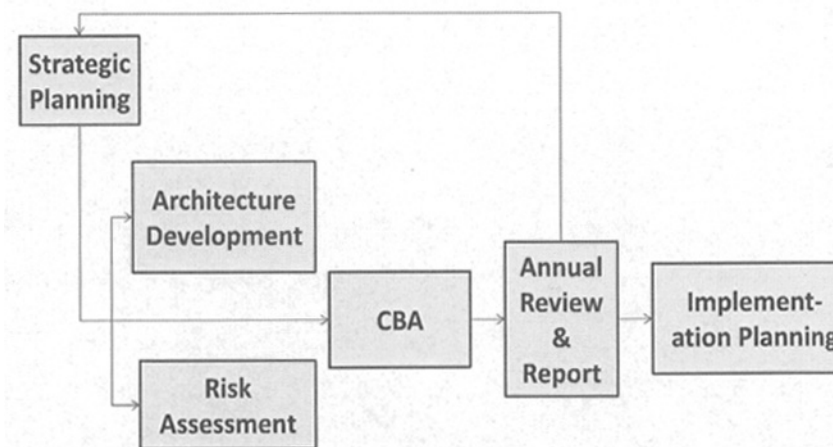
- Status of current detection architecture capabilities.
- Strategic direction for further GNDA enhancements.

Objectives.—The strategic planning, modeling and risk analyses are intended to:

- Reduce the technical and programmatic risk of new efforts.
- Enhance the integration and interoperability of new efforts within the GNDA.

Fiscal Year 2012 Planned Accomplishments/Milestones:

- Annual GNDA development study plan.
- Update GNDA “baseline” architecture.
- Implement Capabilities-Based Assessment (CBA) process:
 - Study plan;
 - Inter-agency working group meetings; and
 - Gaps and solutions.
- Risk-based architecture gaps and solutions prioritization.
- Joint Annual Review and Annual Report.
- Update GNDA strategic plan as required.



RD&O—Systems Engineering and Architecture PPA.—Annual planning, modeling, and analysis, \$5,100,000.

Technology Readiness Level.—N/A—Not a systems development effort.

Timeline for Transition.—N/A—Not a systems development effort.

GNDA Alignment.—GNDA performance goals 1 through 10.

DNDO—GNDA DEVELOPMENT: INTERNATIONAL DOMAIN

Program Description/Objectives

Program Description.—The goal of the international layer is to improve the ability to detect nuclear and other radioactive materials by increasing the national and regional-level detection capability efforts and encouraging the development and implementation of PRND capabilities in other countries. Emphasis is placed on detection efforts in all pathways (air, land, maritime, commercial, and private transportation). International engagement fosters national-level detection architectures in other countries/regions that compliment and reinforce the detection capabilities of the United States.

Objectives:

- Foster bilateral and multi-lateral relationships to enhance national and regional-level architecture development and PRND capabilities.
- Build on USG and international assistance efforts to create a multi-layered rad/nuc detection capability.
- Leverage international engagement efforts to further enhance the domestic implementation of more robust rad/nuc detection architectures that contribute to an expanded GNDA.

Fiscal Year 2012 Planned Accomplishments/Milestones:

- Conduct two “Global Initiative to Combat Nuclear Terrorism Implementation Workshops” to follow on Model Guidelines Document (MGD) development and implementation.
- Conduct one regional GNDA workshop.
- Conduct three regional architectural analyses.

- Continue bilateral and multilateral engagements with key foreign partners on nuclear detection architectures, to include the International Atomic Energy Agency, and Global Initiative to Combat Nuclear Terrorism and other partners.

International GNDA Studies

Work on international geographical architectural analyses to recommend improvements in our national or regional-level detection capacity in foreign countries is expanding.

International engagements are prioritized and conducted in both bilateral and multi-lateral fora through agreements and arrangements (e.g. S&T Agreements, UNSCR 1540, GICNT) and with existing institutions (e.g., IAEA, World Customs Organization, Interpol, International Civil Aviation Organization, International Maritime Organization, etc) as a means to bolster the GNDA.

RD&O—Systems Engineering and Architecture PPA.—GNDA development—international, \$3,530,000.

Technology Readiness Level.—N/A—Not a systems development effort.

Timeline for Transition.—N/A—Not a systems development effort.

GNDA Alignment.—GNDA performance goals 1.1, 1.2, 1.3, and 1.4.

DNDO—GNDA DEVELOPMENT: LAND BORDER DOMAIN

Program Description/Objectives

Program Description.—DNDO develops time-phased strategies and plans for improving the probability of preventing and deterring rad/nuc attacks through the land border pathway. In general, studies will be commissioned to identify and characterize trade-offs, risks, and costs before deciding on specific implementation paths. DNDO works with our front-line end-user components to assess and implement solutions to mitigate these threats.

Objectives:

- Continue to support analyses of detection strategies between the Ports of Entry (POEs) and remaining vulnerabilities at POEs.
- Continue to support modeling and risk assessments focused on characterizing the threat and identifying opportunities for detection and interdiction at the border.

Fiscal Year 2012 Planned Accomplishments/Milestones

Land Border GNDA Requirements Development Studies:

- Complete the Land Border Optimum POE Strategy study.
- Document gaps and priorities based on the Land Border Optimum POE Strategy study and the Probability of Encounter study.

Land Border Pathways:

- Develop supporting documentation (e.g., mission needs statement) for at least one concept, including giving consideration to those concepts for which analysis plans were developed in fiscal year 2011.
- Develop a final report describing radiation detector types, operational procedures, and policy provisions that might be suitable for improving the land border elements of the GNDA.

Land Border GNDA Studies

The Land Border Pathways is an iterative program that leverages existing and emerging technologies and findings from laboratory and field evaluations against capability gaps and mission requirements generated from studies and direct input from user representatives.

Objective.—Continue to support the CBP Office of Border Patrol (OBP) with improvements to its rad/nuc detection capabilities, both in developing the next generation of detectors as well as procuring detectors for OBP, as funds are available.

RD&O—Systems Engineering and Architecture PPA.—GNDA development—Land border pathways, \$3,330,000.

Technology Readiness Level.—N/A—Not a systems development effort.

Timeline for Transition.—N/A—Not a systems development effort.

GNDA Alignment.—GNDA performance goals 2 and 3.

DNDO—GNDA DEVELOPMENT: AVIATION DOMAIN

Program Description/Objectives

Program Description.—This effort determines the bounding requirements for critical Aviation mission area projects to optimize mobility, agility, and adversary cost; to develop holistic airport solutions; and to address International General Aviation (IGA) and domestic general aviation scanning.

Objectives:

- Examine the intersection of International Commercial Aviation (ICA) Pax/Bag, ICA Air Cargo, and IGA pathways, including the commonality of systems and processes that can be leveraged and shared.
- Reduce long-term burdens of system acquisition, maintenance, and operation by seeking cumulative benefits gained from enhanced efficiencies across national and global operations.

Fiscal Year 2012 Planned Accomplishments/Milestones:

- Begin regional, cross-border aircraft vulnerability mitigation analysis of Northern Border and Caribbean aviation traffic.
- Assess feasibility of developing software that will assist operations centers in detecting flight anomalies that pose direct-to-target threats.
- Begin development of IGA security gap solutions (for inbound IGA).
- Complete DHS-AMD-102-1 activities to document capability gaps for domestic APOEs, and document solution options.



RD&O—Systems Engineering and Architecture PPA.—GNDA development—Aviation domain, \$2,470,000.

Technology Readiness Level.—N/A—Not a systems development effort.

Timeline for Transition.—N/A—Not a systems development effort.

GNDA Alignment.—GNDA performance goals 2.1, 2.2, and 5.1.

DNDO—GNDA DEVELOPMENT: MARITIME DOMAIN

Program Description/Objectives

Maritime GNDA Requirements Development Program Description.—Conduct architectural studies and Capability-Based Assessments (CBAs) to ascertain gaps and define the interagency PRND capabilities needed to strengthen maritime pathways against rad/nuc threats (materials, weapons, and conveyances) and formulate recommendations to mitigate waterway/seaport vulnerabilities to achieve the maximum risk reduction within the constraints of the available budget.

Objectives:

- Determine gaps and vulnerabilities.
- Formulate recommendations and plans to deny entry of unauthorized rad/nuc materials and weapons into the United States at seaports, waterways and between POEs.
- Develop a well-coordinated network to integrate the GNDA with the national plan to achieve Maritime Domain Awareness (MDA) and understand inter-relationships within the multi-layered structure of GNDA.

Fiscal Year 2012 Planned Accomplishments/Milestones:

- Continue MDA CBAs that design and integrate maritime PRND data and information into the MDA enterprise-wide network; recommend options that improve small vessel surveillance, detection, analysis, and awareness of incidents and activities.
- Initiate CBA of the cruise line industry (cruise ships and terminal operations).
- Continue maritime modeling and operations analysis framework that integrates a wide range of threats and countermeasures; conduct tradeoff studies to support future planning decisions; and integrate estimates of detection/interdiction probabilities and consequences of attack.

Maritime Capability Development Program Description.—This program builds on lessons learned from the West Coast Maritime Pilot (WCMP) to develop or enhance State, local, and tribal PRND capabilities. Programmatic support includes CONOPS and SOP development, training program assistance, exercise and drill support, and assistance with equipment selection decisions.

Objectives:

- Assist Federal, State, local, and tribal government stakeholders and area maritime security committees on operational protocols, training, and exercises that support small vessel PRND capabilities.
- Assess geographic port configurations to maximize interdiction.
- Improve scanning of small maritime craft by planning to increase detection systems for maritime forces.
- Increase port security grant requests for PRND programs.

RD&O—Systems Engineering and Architecture PPA.—GNDA development—Maritime domain, maritime PA, \$3,350,000.

Technology Readiness Level.—N/A—Not a systems development effort.

Timeline for Transition.—N/A—Not a systems development effort.

GNDA Alignment.—GNDA performance goals 2 through 10.

DNDO—GNDA DEVELOPMENT: INTERIOR DOMAIN

Program Description/Objectives

Program Description.—Guided by the GNDA, DNDO supports the assessment and mitigation of threats in the land borders, aviation, maritime and interior mission areas through the development of specific architecture studies, CONOPS analyses, detector modeling studies, and enterprise architecture support that are specific to each mission area. These studies typically focus on specific programs and directly support DNDO pilot and Research and Development (R&D) initiatives. These preliminary studies are intended to reduce the technical and programmatic risk of new efforts and enhance their integration and interoperability with the overall GNDA.

Objectives:

- Determine gaps and vulnerabilities and formulate recommendations and plans to mitigate them.
- Develop a well-defined and carefully coordinated network of interrelationships by studying the multi-layered structure of the rad/nuc detection architecture.

Fiscal Year 2012 Planned Accomplishments/Milestones:

- Conduct three foundational analyses on the application of PRND capabilities, including whether or where to employ 100 percent or randomized screening concepts at strategic locations. Three studies related to the domestic layer are expected to be completed by the end of fiscal year 2012.
- Continue work on detection modeling, data fusion, and analysis to enhance detection capabilities in support of various fixed and mobile operational detection programs and in the support of “surge” operations.

Interior Studies:

- DNDO will focus efforts to develop capabilities to detect threats with limited or imperfect intelligence.
- These capabilities rely on the multiple State and local law enforcement agencies that are available to perform rad/nuc detection operations using mobile and human-portable sensors.
- USG surge efforts will require interactions with relevant State and local and Federal agency activities to develop coordinated architectures and CONOPs.
- Foundational architecture analyses will be performed to identify and prioritize PRND capabilities and deployment and search strategies based on the effectiveness of each.

RD&O—Systems Engineering and Architecture PPA.—GNDA development—Interior domain, \$1,680,000.

Technology Readiness Level.—N/A—Not a systems development effort.

Timeline for Transition.—N/A—Not a systems development effort.

GNDA Alignment.—GNDA performance goals 2 through 10.

DNDO—S&L INITIATIVES RAD/NUC CHALLENGE

Program Description/Objective

Program Description.—The SAFE Port Act charges DNDO with enhancing and coordinating the nuclear detection efforts of Federal, State, and local officials in order to ensure a managed, coordinated adjudication of rad/nuc threats.

DNDO is promoting an opportunity to emphasize the rad/nuc detection capabilities and operations at the State, local, and tribal levels through a competition among the PRND community, with industry demonstrations and information exchange forums.

Objective.—Measurably advance the operational expertise and technical capabilities of those assets that would be involved in coordinated surge or intelligence informed deployments.

Fiscal Year 2012 Planned Accomplishments/Milestones

Competition Rodeo.—Creates productive, spirited competition among individuals and teams at all levels of the PRND community.

Information Exchange Forum.—Scheduled activities including workshops, briefings, panel meetings, and the presentation of case studies and other papers sponsored by members of the PRND community who wish to share their lessons learned, ideas, and insights.

System/Capability Expo.—Includes exhibit booths, system, and CONOPS demonstrations, hands-on experiences, and showcases.

Projected Outcomes:

- Sharing of successes and lessons learned.
- Shaping independent research and development programs by exposing industry and academia to the Government's needs and upcoming opportunities.
- Encouraging a dialog between the equipment development community and State, local, and tribal law enforcement and first responders involved in PRND.
- Fostering more effective community-wide competition and advancement by establishing a greater awareness of the current state-of-the-art technology and CONOPS.

RD&O—Systems Development PPA.—Rad/Nuc challenge, \$2,630,000.

Technology Readiness Level.—N/A—Not a systems development effort.

Timeline for Transition.—N/A—Not a systems development effort.

GND Alignment.—GND performance goals 4 and 7.

DNDO—HUMAN PORTABLE TRIPWIRE (HPT)

Program Description/Objective

Program Description.—Investigates the technology around small, wearable systems that provide passive monitoring capability to increase the likelihood of detecting rad/nuc material through constant, nondeliberate rad/nuc scans. HPT detection system should be considered standard operating equipment capable of being worn by key operators at all times, cost-effective and deployed to a large number of operators to increase the opportunity for detection.

The proposed HPT concept has improved performance and added capabilities over Commercial Off-the-Shelf (COTS) personal radiation detectors currently used by law enforcement in the field. Additionally, it will have capabilities such as isotope identification and data communication. The device will also have the capability of “wired” and “wireless” interface to networks, laptops, satellite phones, and other devices as required. HPT will build on lessons learned from the Intelligent Personnel Radiation Locator Advanced Technology Demonstration, in addition to many other support COTS technologies such as handheld data processor devices, communications and data transfer.

Fiscal Year 2012 Planned Accomplishments/Milestones:

- Initiate the development of an HPT system designed to meet user requirements.
- Conduct data collection efforts against Special Nuclear Material (SNM) to improve algorithm performance of HPT systems.
- Conduct an Early Operational Assessment of the HPT system in a simulated operational environment.

Objectives.—Develop a low-cost approach to increase passive, nondeliberate detection, and provide spectroscopic identification and data transfer.



RD&O—Systems Development PPA.—HPT, \$9,060,000.

Technology Readiness Level:

—Basic Technology Readiness Level (TRL) is 9.

—Application to this mission is at TRL 4.

Timeline for Transition.—Transition to full-scale development, TRL 7, is funding dependant, but considered feasible by 2014.

GNDA Alignment.—GNDA performance goals 2.1, 2.2, 5.1, 6.1, and 6.3.

DNDO—CARGO IMAGING FOR SHIELDED NUCLEAR THREATS (CISNT)

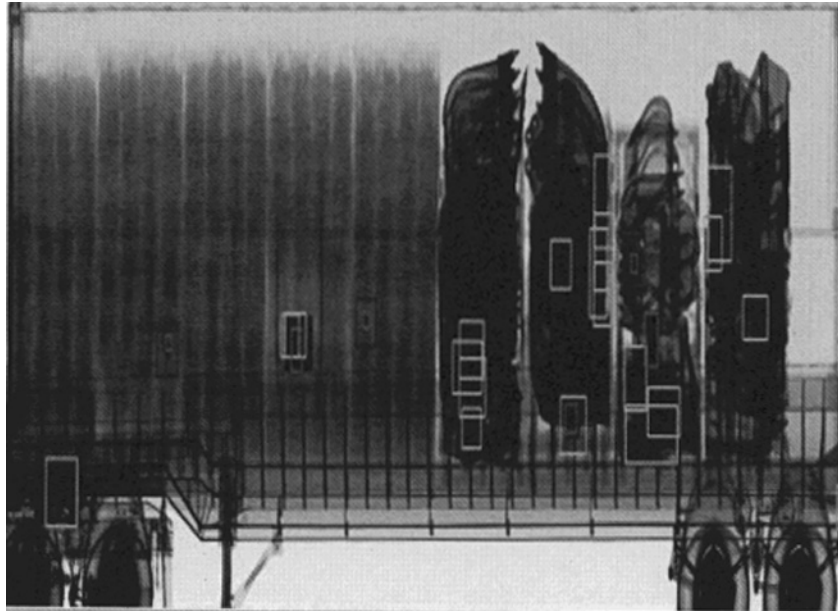
Program Description/Objective

Program Description.—Program will evaluate and develop as appropriate non-intrusive inspection radiography capability that can identify and discriminate special nuclear materials and shielded material contained in full-size trucks, cargo containers, and rail cars. In doing so, CISNT will leverage the findings from past and current Transformational Applied Research programs. This program was initiated as the Advanced Cargo Imaging program and included in the President's budget request for fiscal year 2011. The name change reflects the objectives of the program.

Objective.—To develop a capability to identify shielded nuclear material in cargo to act as a companion capability with passive radiation portal monitors.

Fiscal Year 2012 Planned Accomplishments/Milestones:

- Refine operational requirements and perform an Analysis of Alternatives (AOA).
- Begin the Technology Demonstration and Characterization (TD&C) process for a selected set of systems; collect data to characterize the operational environment; and determine the limits of technical approach.
- Complete draft AOA for CISNT.
- Continue to evaluate competing alternatives.
- Develop an operational requirements document leveraging lessons learned from previous related programs and TD&C.



RD&O—Systems Development PPA.—CISNT, \$13,470,000.

Technology Readiness Level:

—Basic TRL is 9.

—Application to this mission is at TRL 6.

Timeline for Transition.—Transition to full-scale development, TRL 7, is funding dependant, but considered feasible by 2013.

GNDA Alignment.—GNDA performance goals 2.1, 2.2, 6.1, and 6.3.

DNDO—LONG-RANGE RADIATION DETECTION (LRRD)

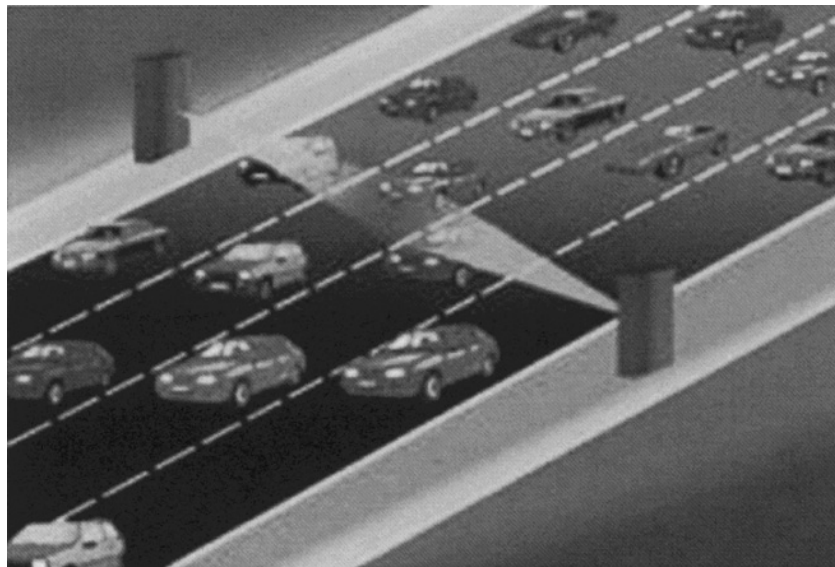
Program Description/Objective

Program Description.—Determine if a passive long-range rad/nuc detection system should be developed and fielded, building upon technologies demonstrated by Stand-Off Radiation Detection System and Roadside Tracker. To avoid redundancies with preexisting programs, LRRD is focused on Interior needs and stakeholders.

Objective.—Provide detectors with better sensitivity, and with ability to identify and localize sources.

Fiscal Year 2012 Planned Accomplishments/Milestones:

- Develop operational requirements document.
- Develop concepts of operations.
- Develop integrated logistics support plan.
- Develop the acquisition program baseline.
- Develop the LRRD test and evaluation master plan.
- Finalize LRRD limited use experiment final report.



RD&O—Systems Development PPA.—LRRD, \$5,480,000.

Technology Readiness Level.—TRL will be assessed as part of stage 2a.

Timeline for Transition.—Stage 2a scheduled for fiscal year 2012.

GNDA Alignment.—GNDA performance goals 4.1 and 5.1.

DNDO—INTERNATIONAL RAIL PROGRAM

Program Description/Objective

Program Description.—International Rail is referenced in Public Law 110–28 and Public Law 110–53. Previous efforts characterized the rail operating environment, identified user needs, conducted stream of commerce data collection efforts at a lower volume Port of Entry (POE) site, and conducted evaluations of architecture alternatives. Current efforts are focused on an additional stream of commerce characterization, Acquisition Management Directive 102–01 documentation development, and detector testing.

Objective.—Develop implementable solution to detect and identify illicit rad/nuc materials entering the United States via freight rail cargo through the 31 POEs identified in the Trade Act of 2002.

Fiscal Year 2012 Planned Accomplishments/Milestones:

- Complete an analysis of alternatives for the Rail Cargo Scanning project for International Rail.
- Continue implementation of any cooperative project(s) identified as working in concert with Second Line of Defense.
- Document—in concert with CBP—lessons learned from operational experiences with rad/nuc detection system(s) utilizing passive and active detection at rail crossings.
- Document the performance of candidate international rail systems.



RD&O—Systems Development PPA.—International rail, \$3,120,000.

Technology Readiness Level.—No specific technology has been identified for this mission; TRL is undetermined.

Timeline for Transition.—Identification of appropriate technology and its transition to full-scale development, TRL 7, is projected to occur by 2015.

GNDA Alignment.—GNDA performance goals 2.1, 2.2, and 9.3.

DNDO—ON-DOCK RAIL PROGRAM

Program Description/Objective

Program Description.—The On Dock Rail Program analyzes alternative solutions for scanning the 2 percent of intermodal cargo containers arriving in the United States via ship that are directly transferred to rail cars at the ports. These containers are currently being scanned by mobile radiation portal monitors, which involves a time-consuming process of unstacking and restacking the containers. The other 98 percent of ship cargo is transferred directly to trucks which are subsequently scanned at the exit gates by radiation portal monitors.

Objective.—To develop a capability to effectively and efficiently scan containerized cargo that is transferred directly from ship to rail at sea ports of entry, without an adverse impact to the flow of commerce.

Fiscal Year 2012 Planned Accomplishments/Milestones:

- Collect straddle portal prototype stream-of-commerce data.
- Complete alternatives analysis.
- Perform the system engineering review.
- Transition from requirements and alternatives analysis to solution development.



RD&O—Systems Development PPA.—ODR, \$10,280,000.

Technology Readiness Level:

—Basic TRL is 7.

—Application to this mission is TRL 7.

Timeline for Transition.—Transition to full-scale development is projected to occur in 2012.

GNDA Alignment.—GNDA performance goals 2.1, 2.2, 6.1, and 6.3.

DNDO—SMALL VESSEL STANDOFF DETECTION PROGRAM (SVSD)

Program Description/Objectives

Program Description.—Seeks to develop and field a capability to provide standoff boat-to-boat, aerial, and fixed-site rad/nuc detection systems in U.S. port areas and maritime regions. This program will address the need of Federal, State, and local maritime officers to conduct PRND screening missions against the small vessel threat without the need to board each encountered vessel.

Objectives:

—Initially develop a capability for scanning small vessels from maritime law enforcement vessels on the water.

—Follow-on projects will address aerial and land-based deployment of sensors to complement the boat-to-boat system.

Fiscal Year 2012 Planned Accomplishments/Milestones:

—Complete Acquisition Management Directive (AMD) 102–01 activities to receive milestone 2B approval for boat-to-boat systems. Systems delivered to USCG and CBP Office of Air and Marine for operational evaluation.

—Complete AMD 102–01 activities to receive milestone 1 approval for aerial-mounted systems.



RD&O—Systems Development PPA.—SVSD, \$6,610,000.

Technology Readiness Level.—TRL will be assessed as part of stage 2a.

Timeline for Transition.—Stage 2a scheduled for fiscal year 2014.

GNDA Alignment.—GNDA performance goals 3.2 and 5.1.

DNDO—NON-HELIUM 3 (^3He) NEUTRON DETECTION ALTERNATIVES PROGRAM

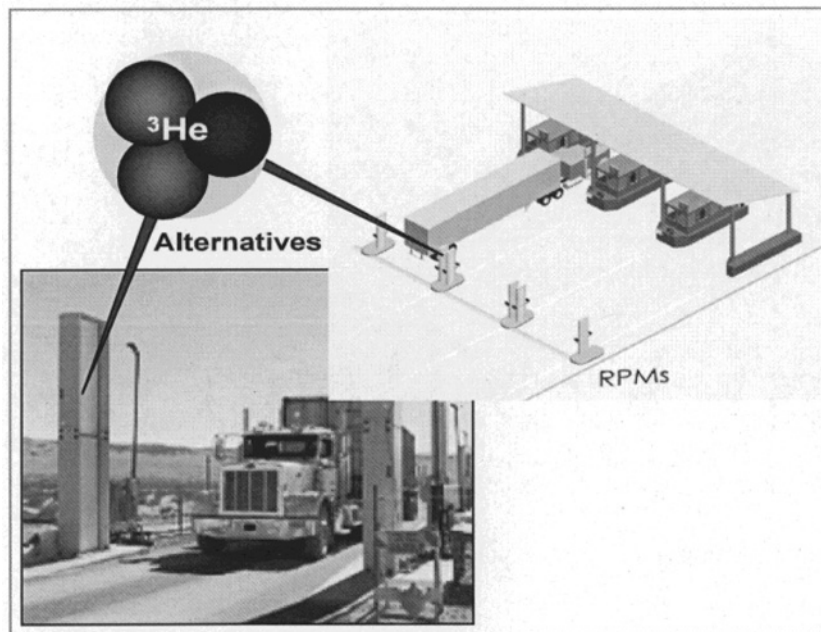
Program Description/Objective

Program Description.—Addresses the impact of the shortage of Helium-3 (^3He) upon the cost and availability of rad/nuc detection systems. Current efforts are focused on the Neutron Detector Replacement Project (NDRP), qualifying near-term technologies as suitable to replace ^3He for Neutron Detection Modules (NDM) in various applications, including Radiation Portal Monitor Systems (RPMS) and back-pack systems.

Objective.—To develop cost-effective alternatives to ^3He for broad-based neutron detection applications.

Fiscal Year 2012 Planned Accomplishments/Milestones:

- Conduct market research and release a Request for Information (RFI) on back-pack systems under development for commercial application using non- ^3He -based neutron detectors.
- Conduct testing of products responding to the RFI and release results of tests to vendors to accelerate non- ^3He based neutron detection technology for back-pack systems.



RD&O—Systems Development PPA.—Neutron detector replacement, \$5,180,000.

Technology Readiness Level.—Several TRL 6 and 7 approaches are available.

Timeline for Transition.—Transition of selected approaches to full-scale development is funding dependant.

GNDA Alignment.—GNDA performance goals 2.1, 3.1, 5.1, and 6.1.

DNDO—AVIATION MULTI-PATHWAY SCANNING INTEGRATION

Program Description/Objective

Program Description.—The first component of the program is the holistic airport deployments effort, which examines International Air Cargo (IAC) and International General Aviation (IGA) pathways at domestic air POEs. The second component involves evaluating the feasibility of using Computed Tomography (CT) and Advanced Technology (AT) x ray systems, currently deployed throughout aviation pathways to detect explosives, to detect rad/nuc materials in baggage and small cargo.

Objective.—Identify options for the aviation pathway to leverage existing capabilities, and to improve deterrence against aviation threats.

Fiscal Year 2012 Planned Accomplishments/Milestones:

- Complete analysis for the deployment of RPMs to a limited number of APOEs for targeted air cargo scanning.
- Initiate Analysis of Alternatives (AoA) process for APOEs, addressing the full scope of APOE operations.
- Initiate modeling/simulation activities to support AoA process.
- Initiate characterization testing of detection systems to support AoA process and modeling/simulation activities.
- Pending feasibility results of baseline CT/AT tests, continue partnering with S&T and TSA on path forward.



RD&O—Systems Development PPA.—Aviation multi-pathway scanning integration, \$9,660,000.

Technology Readiness Level.—TRL will be assessed as part of stage 2a.

Timeline for Transition.—Stage 2a scheduled after fiscal year 2016.

GNDA Alignment.—GNDA performance goals 1.2, 2.1, 2.2, 3.1, 4.1, 5.1, and 9.3.

DNDO—ALGORITHM IMPROVEMENT

Program Description/Objectives

Program Description.—Improves overall mission performance of algorithms employed in rad/nuc detection and reporting systems. The current effort focuses on developing, deploying and maintaining the DHS isotope ID reach-back analysis tool, which enables field agents to quickly and easily engage on-call scientific experts to identify isotopes that cannot be identified on location. Current efforts also include energy windowing and injection studies. Future efforts are planned to drive the creation of more robust algorithms by challenging industry partners to identify specific isotopes against known spectra and have the ability to score their performance.

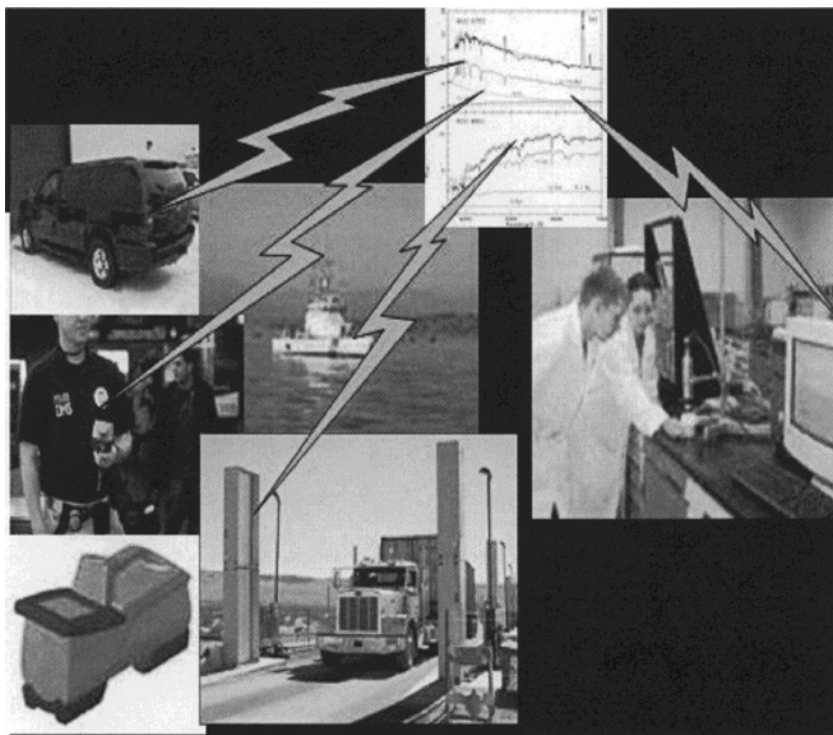
Objectives:

—To cost effectively ensure that rad/nuc detection algorithms are improved to remain current with emerging technologies and concepts of operations.

- Provide an infrastructure that makes gamma spectra benchmarks available to develop new (or upgrade) isotope identification algorithms while allowing the Government to score algorithms objectively.

Fiscal Year 2012 Planned Accomplishments/Milestones

- Define benchmarks to measure algorithm performance.
- With High-Purity Germanium (HPGe) and Sodium Iodide (NaI) detectors, collect and validate source spectra for open and closed benchmark data sets to develop new algorithms and score existing ones.
- Promulgate benchmarks throughout Government, assess existing algorithms, and target improvements.
- Define algorithm replay tool interface requirements, reference electronic packages, isotopes of interest, and algorithm scoring criteria.



RD&O—Systems Development PPA.—Algorithm improvement, \$4,200,000.

Technology Readiness Level.—Basic TRL is 9.

Timeline for Transition.—Initial solutions are deployed. Spiral advancements continue.

GNDA Alignment.—GNDA performance goals 2.1, 3.1, 5.1, and 6.1.

DNDO—TEST AND EVALUATION OPERATIONS

Program Description/Objectives

Program Description.—Provide operational capabilities needed to plan and execute the DNDO test and evaluation program. Capability includes working with subject matter experts from national laboratories to ensure scientifically defensible test designs and engineering support to plan and execute tests, including formal test milestone reviews, oversight of field test activities, and analysis support to evaluate performance and write test high-quality reports.

Objectives:

- Develop timely and credible test and evaluation campaigns in support of internal and external (international, Federal, State, local, and other entities) customers' rad/nuc detection requirements.

—Develop repeatable, evolutionary, and controlled processes for planning and conducting tests.

Fiscal Year 2012 Planned Accomplishments/Milestones

- Maintain the expertise and resources necessary to plan and execute up to 15 individual test campaigns.
- Document formal test milestone reviews.
- Issue test reports within 90 days of completion of data validation.



RD&O—Assessments PPA.—T&E operations, \$8,390,000.

Technology Readiness Level.—N/A—Not a systems development effort.

Timeline for Transition.—N/A—Not a systems development effort.

GNDA Alignment.—GNDA performance goal 9.3 (also supports 3.1, 3.2, and 5.1).

DNDO—TEST AND EVALUATION INFRASTRUCTURE

Program Description/Objectives

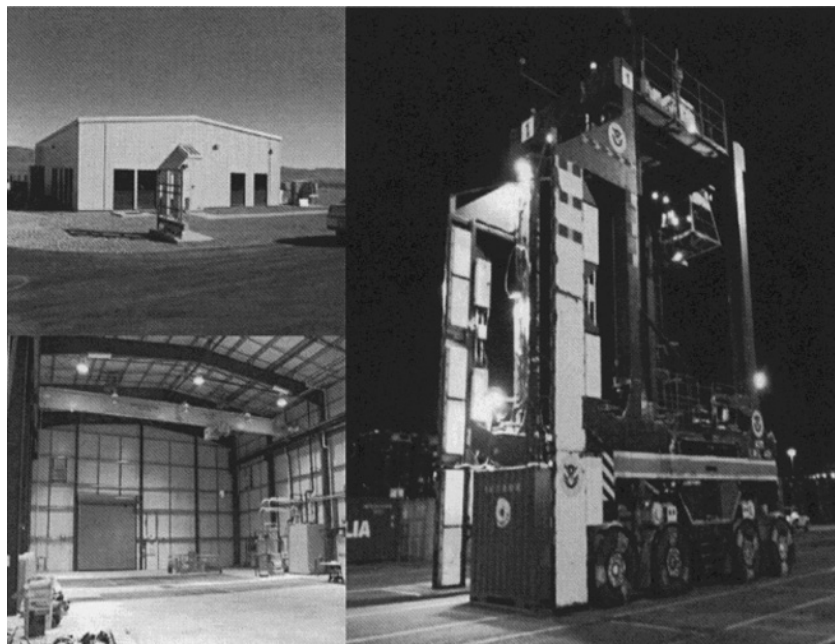
Program Description.—Provide development, operation, and maintenance of the infrastructure required to execute DNDO test and evaluation efforts including facilities, technical support staff, test equipment, data collection technology, and design and fabrication of special nuclear material (SNM) test objects. DNDO test facilities include the Rad/Nuc Countermeasures Test and Evaluation Complex (RNCTEC) at the Nevada National Security Site (N2S2), the Rail Test Center (RTC) at the Port of Tacoma, and other limited-term infrastructure needs at test locations across the national laboratory complex.

Objectives:

- Establish and develop an integrated T&E infrastructure of facilities, equipment, test objects, processes, and personnel to meet U.S. Government rad/nuc T&E needs.
- Engage the multi-agency rad/nuc community for future test instrumentation and infrastructure needs.
- Design and fabricate appropriate special nuclear material (SNM) and radiological sources and materials for realistic threat-based testing.

Fiscal Year 2012 Planned Accomplishments/Milestones:

- O&M of RNCTEC and RTC.
- Continue physical security upgrades, including procurement and deployment of sensors, vehicle barriers, and perimeter fencing to RNCTEC to reduce costs for force protection in preparation for testing activities using category I and II SNM sources.
- Complete fabrication SNM test sources:
 - Two additional sizes (#3 and #4) of HEU spheres;
 - Two reactor grade Pu sealed sources; and
 - Four additional sizes of weapons grade Pu sealed sources.



RD&O—Assessments PPA.—T&E infrastructure, \$9,500,000.
Technology Readiness Level.—N/A—Not a systems development effort.
Timeline for Transition.—N/A—Not a systems development effort.
GNDA Alignment.—GNDA performance goal 9.3.

DNDO—T&E DATA MANAGEMENT AND ALGORITHM TEST BED

Program Description / Objectives

Program Description.—Provides for the collection, analysis, reporting, and archiving of test data collected during DNDO test campaigns, as well as the collection of similar test reports by other agencies. Includes maintaining and enhancing two data management systems: Archive and Retrieval Management System (ARMS) and Report Analysis and Archive System (RAAS).

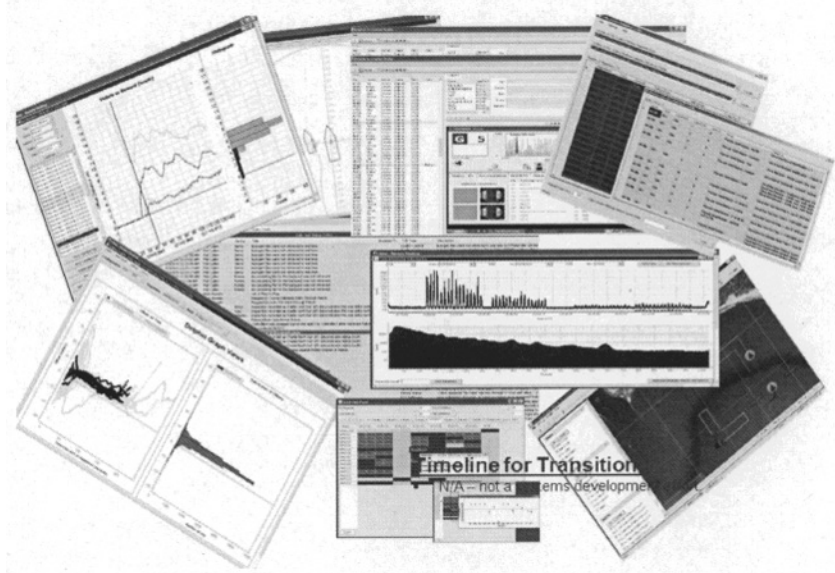
The Algorithm Test Bed (ATB) provides the capability to evaluate the baseline performance of detector algorithms, and compare new and existing detector algorithms against standardized sets of both modeled and measured threats in a virtual environment.

Objectives:

- Develop an independent and peer-reviewed framework for evaluating performance of detection and identification algorithms for all handheld, mobile, and fixed systems against realistic operational threats.
- Develop, operate and maintain the ARMS and the RAAS.

Fiscal Year 2012 Planned Accomplishments / Milestones:

- Continue to perform ATB studies that allow programs to make informed program-wide decisions for increased performance and deployment of detection systems.
- Accept spectroscopic algorithms from developers and assess using the generic algorithm test bed.
- Review, evaluate, and add 150 radiation and radiograph reports to expand the content of RAAS.
- Continue information sharing of test data, analysis, studies, and tools to expand the content and capabilities of ARMS across the DNDO user community and with peer organizations.



RD&O—Assessments PPA.—T&E data management and algorithm test bed, \$4,200,000.

Technology Readiness Level.—N/A—Not a systems development effort.

Timeline for Transition.—N/A—Not a systems development effort.

GNDA Alignment.—GNDA performance goals 3.1, 3.2, 5.1, and 9.3.

DNDO—TEST AND EVALUATION DIRECTED TEST

Program Description/Objectives

Program Description.—Planning and execution of test campaigns to characterize currently available equipment in operationally relevant environments and CONOPS to inform State and local entities in the development of effective Preventive Radiological/Nuclear Detection (PRND) programs at the State, local, and tribal level.

Objectives:

- Provide comprehensive performance data on rad/nuc detection systems, based on operationally relevant threats and scenarios, to State, local, and tribal users.
- Provide opportunities for State, local, and tribal users to learn from hands-on operation of rad/nuc detections systems against actual SNM threat sources in operationally relevant conditions and scenarios.

Fiscal Year 2012 Planned Accomplishments/Milestones:

- Complete test and final report for Gryphon test campaign to inform Federal, State, and local operational entities of the performance of aerial detection systems.
- Complete testing and produce joint EU/US ITRAP+10 report.
- Initiate the next directed test dependent on highest priority determined in fiscal year 2011.



RD&O—Assessments PPA.—T&E directed test, \$4,810,000.
Technology Readiness Level.—N/A—Not a systems development effort.
Timeline for Transition.—N/A—Not a systems development effort.
GNDA Alignment.—GNDA performance goals 4.1 and 9.3.

DNDO—GRADUATED RAD/NUC DETECTOR EVALUATION AND REPORTING (GRADERSM)

Program Description / Objectives

Program Description.—Provide a vendor-driven framework to independently test commercially available radiation detection and identification products against standards to help Federal, State, and local stakeholders make informed PRND equipment procurements.

Objectives:

- Standardize instrument testing and test results reporting to assure valid comparisons.
- Inform State, local, and tribal entities on performance of COTS systems in making FEMA grant purchases of rad/nuc detection systems.
- Encourage vendors to develop better radiation detection and identification products.

Fiscal Year 2012 Planned Accomplishments / Milestones:

- Initiate Phase II of GRaDER and begin testing against Technical Capability Standards.
- Continue Phase I of the GRaDER program for manufacturer-financed testing of COTS rad/nuc detection systems by National Voluntary Laboratory Accredited Program accredited laboratories.
- Maintain the GRaDER Evaluated Equipment List on the FEMA Responder Knowledge Base.
- Begin implementing the GRaDER postmarket surveillance program to verify continued compliance for previously tested COTS instruments.

RD&O—Assessments PPA.—GRaDER, \$820,000.

Technology Readiness Level.—N/A—Not a systems development effort.

Timeline for Transition.—N/A—Not a systems development effort.

GNDA Alignment.—GNDA performance goals 4.1 and 9.3.

DNDO—PRND PILOT PROGRAMS

Program Description / Objectives

Program Description.—Provide a defensible and repeatable framework to evaluate operational utility of mature rad/nuc detection technology in new operational environments. Assists users to establish venue specific CONOPs and procedures, command and control, and technical reachback protocols. Provides an initial set of appropriate rad/nuc detection systems to establish an initial operating capability.

Objectives.—Develop and execute a repeatable and defensible pilot program that provides technical and operational assessments resulting in the transition of new and improved operational capabilities for preventative rad/nuc detection to Federal, State, local, and tribal users.

Fiscal Year 2012 Planned Accomplishments / Milestones.—In coordination with stakeholders, conduct a series of exercises including drills, functional exercises, and full-scale exercises to train, test and evaluate CONOPS. Training and equipment deployed during the pilot will be provided to the stakeholders.



RD&O—Assessments PPA.—PRND pilot programs, \$3,930,000.

Technology Readiness Level.—N/A—Not a systems development effort.

Timeline for Transition.—N/A—Not a systems development effort.

GNDA Alignment.—GNDA performance goals 2.1, 3.1, 4.1, 5.1, and 9.3.

DNDO—RED TEAM AND NET ASSESSMENTS

Program Description / Objective

Red Team Program Description.—Conducts adversarial-based assessments from an outside perspective without using any “inside” information of current or planned capabilities. Executes overt and covert tests to intentionally introduce radioactive sources against known defenses to assess the performance of fielded technology, training, and protocols.

Net Assessments Program Description.—Assesses the effectiveness of planned and deployed elements of the GNDA and supporting programs.

Objective.—Identify vulnerabilities and best practices in deployed PRND systems and DNDO programs to include technologies, procedures, training, and communication pathways.

Fiscal Year 2012 Planned Accomplishments / Milestones

Fiscal Year 2012 Focus.—Under IAW Director DNDO Guidance, RTNA will work to increase support to State and local PRND programs.



RD&O—Assessments PPA.—RTNA, \$11,460,000.

Technology Readiness Level.—N/A—Not a systems development effort.

Timeline for Transition.—N/A—Not a systems development effort.

GNDA Alignment.—GNDA performance goals 2.1, 3.1, 3.2, 4.1, 7.3, and 9.2.

DNDO—JOINT ANALYSIS CENTER (JAC)

Program Description / Objective

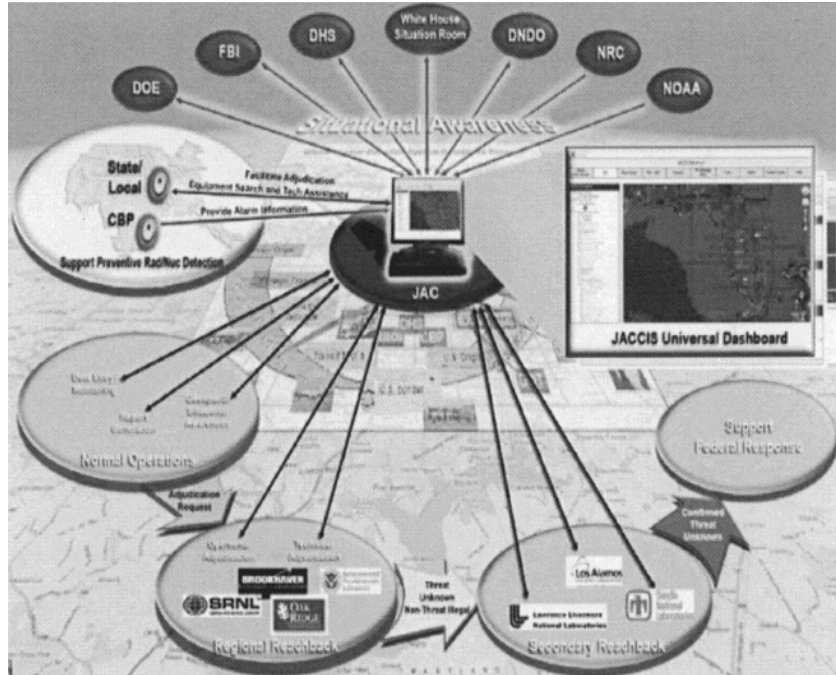
Program Description.—Interagency coordination mechanism and central monitoring point for the Global Nuclear Detection Architecture, maintains situational awareness for the GNDA—to include status of radiological and nuclear (rad/nuc) detection assets, visibility into the status of rad/nuc alarms, and awareness of rad/nuc-related incidents and events.

Secondary Reachback (SRB).—Accurate and actionable assessments of illicit nuclear trafficking events and trends, the credibility of nuclear threat communications and other nuclear terrorism indicators. The project serves DNDO's entire community of interest and also provides deep dive on topics of interest for internal use.

Objective.—To provide integrated and centralized alarm adjudication, data collection, and information sharing services.

Fiscal Year 2012 Planned Accomplishments / Milestones:

- Sustained capability.
- Service metrics (as applicable).
- Responsiveness to adjudication, responsiveness to RFI, proactive event situational awareness, rapid situational awareness of given incidents.
- Support the radiation detection community with rapid spectral data analysis and reports.
- Prepare up to 10 technical reports that inform PRND community on detector performance, detection phenomena trends, triggers that may indicate threat material is present and operational aspects of detector performance.



RD&O—Operations Support PPA.—JAC Ops, NAP, and SRB, \$15,850,000.

Technology Readiness Level.—This is an analytical capability in place, TRL 8.

Timeline for Transition.—Sustained capability.

GNDA Alignment.—GNDA performance goals 4.1, 4.2, 5.2, 6.1, 6.2, 6.3, 6.4, 7.1, 7.2, 10.1, 10.2, and 10.3.

DND—JAC COLLABORATIVE INFORMATION SYSTEM (JACCIS)

Program Description/Objectives

Program Description.—To maintain threat-space awareness and execute the operational analysis and reporting function of the Global Nuclear Detection Architecture.

Goals.—Analyze, process, and synthesize information collected through all detection mechanisms and related intelligence.

Objectives:

—Assist State, local, and tribal governments in analyzing and reporting on any unauthorized nuclear and radiological materials in their jurisdictions.

—Process and synthesize information collected through detection mechanisms.

—Receive information from, and disseminate information to relevant authorities.

Fiscal Year 2012 Planned Accomplishments/Milestones:

—Complete development.

—Testing (OT).

—System migration (SPAWAR to DC2).

—Test bed migration to DC-2.

Key performance parameters	Baseline	
	Threshold	Objective
#1 Simultaneous users	15 users	75 users
#2 Number of Detector Systems Connected	1	2
#3 Number of Situation Awareness Display Systems Connected	1	2
#4 Mean Time Between Operational Failure (MTBF) (Minimum of 1 year of monitoring to verify threshold. To be annually assessed.).	4,000 hours (approximately 5.6 months).	20,000 hours (approximately 2.3 years)

Key performance parameters	Baseline	
	Threshold	Objective
#5 Operational Availability	99%	99.9%

RD&O—Operations support PPA.—JACCIS, \$5,030,000.

Technology Readiness Level:

—All COTs software, DHS Technology Reference Model (TRM) approved TRL8.

—Basic TRL is 8.

Timeline for Transition:

—JACCIS program delivered to user in second quarter fiscal year 2011.

—IOC—fiscal year 2011 third quarter.

—Formal operational testing is planned for first quarter fiscal year 2012.

GNDAs Alignment:

—GNDAs performance objectives 1, 2, 3, and 4.

—GNDAs performance goals 4.1, 4.2, 5.2, 7.1, 7.2, and 8.1.

DNDO—PRND TRAINING AND EXERCISES PROGRAM

Program Description/Objectives

Program Description.—The Training and Exercises Program develops and implements rad/nuc training and exercise execution for Federal, State, and local law enforcement and public safety professionals to increase PRND operational capabilities.

Objectives.—The program's main objectives are:

—Increase operational capabilities for Federal, State, and local users.

—Develop and exercise protocols and standards for effective use of radiation detection equipment and associated alarm resolution and reporting processes.

—Develop training curricula for emerging detection technologies.

—Foster organic capabilities by assisting Federal, State, and local agencies in institutionalizing training courses in their academies.

—Support national security special events, DHS special events, and elevated threat conditions, as required.

Fiscal Year 2012 Planned Accomplishments/Milestones:

—Computer Based Training (CBT) for PRD and RIIDs in July 11.

—Complete curricula for mobile systems (PRDs, RIIDs, backpacks, vehicle model) and fixed systems by end of calendar year 2012.

—Annually:

—Directly and indirectly train 5,000 participants in RN detection operations.

—Assist States in establishing PRND exercise programs.

—Participate in the Federal national level exercise.

—Provide domestic State and local exercise support as requested.



RD&O—Operations Support PPA.—PRND training and exercises, \$8,100,000.

Technology Readiness Level.—These are current services, TRL 8.

Timeline for Transition.—Services currently in-place, improving and expanding over time.

GND Alignment.—GND performance objectives 1, 2, 3, and 4.

DNDO—INTERIOR CAPABILITY DEVELOPMENT (ICD)

Program Description/Objectives

Program Description.—The interior capability development program utilizes various levels of engagement and program assistance to develop PRND capability among State, local, and tribal jurisdictions. Our goal is to provide program assistance and engagements that work with all other jurisdictions.

The SLSWG supports the development of DNDO programs and products and serves as the principle collaboration opportunity for members of the PRND community to share best practices and lessons learned.

Objectives.—To catalyze and increase PRND capability nationwide, thereby increasing probability of encountering and detecting rad/nuc materials.

Fiscal Year 2012 Planned Accomplishments/Milestones.—The National Capitol Region is on the verge of purchasing approximately \$3.5 million worth of PRND equipment using HSPG funds and standing up a regional data sharing network for alarm adjudication and tracking. Through facilitated workshops, subject matter expertise, and lessons learned from other programs across the Nation, DNDO is enabling the NCR to execute a program that meets the specific jurisdictional needs that is also interoperable with other Federal, State, and local PRND programs.



RD&O—Operations Support PPA.—Interior capability development, \$5,120,000.

Technology Readiness Level.—This is a current program development service.

Timeline for Transition.—Currently engage in ICD activities in Florida, Georgia, South Carolina, Virginia, North Carolina, Tennessee, Kentucky, Texas, Arizona, New Mexico, California, and Washington, and reaching out to other States and cities interested in developing PRND capabilities.

GNDA Alignment.—GNDA performance objectives 4.1, 4.2, and 7.1.

DNDO—MOBILE DETECTION DEPLOYMENT PROGRAM (MDDP)

Program Description / Objectives

Program Description.—In conjunction with DOE/Radiological Assistance Program (RAP), provide Mobile Detection Deployment Program (MDDP) assets as a national nuclear detection “surge” capability to provide increased security in periods of heightened alert or if specific threats are identified. There are currently five MDDP response systems collocated with DOE RAP teams.

Objectives.—To develop specialized capabilities to augment State and local operations, and to foster and develop comprehensive, integrated, and regional approaches to PRND programs, including surge and intelligence informed events.

Fiscal Year 2012 Planned Accomplishments / Milestones.—Upgrade three small mddp systems and add additional equipment. Additional funds requested to upgrade RIIDS as part of fiscal year 2012 S&L options.

Relevant R&D Programs:

- Human-portable systems (including tripwire).
- Long-range radiation detection program.
- PRND target capability and NIMS resource typing.
- ³He alternative development.



RD&O—Operations Support PPA.—MDDP (sustainment), \$2,740,000.

Technology Readiness Level.—MDDP is a current operational support capability, TRL 8.

Timeline for Transition.—Five MDDUs will be operational and stationed across the Nation by the end of fiscal year 2011.

GNDA Alignment.—GNDA performance objectives 5.1 and 5.2.

DNDO—NTNFC—TECHNOLOGY ADVANCEMENT

Program Description / Objectives

Program Description.—National Technical Nuclear Forensics Center (NTNFC) leads the development of the USG capability to rapidly, accurately, and credibly identify the origin and history of rad/nuc materials obtained or intercepted before a detonation.

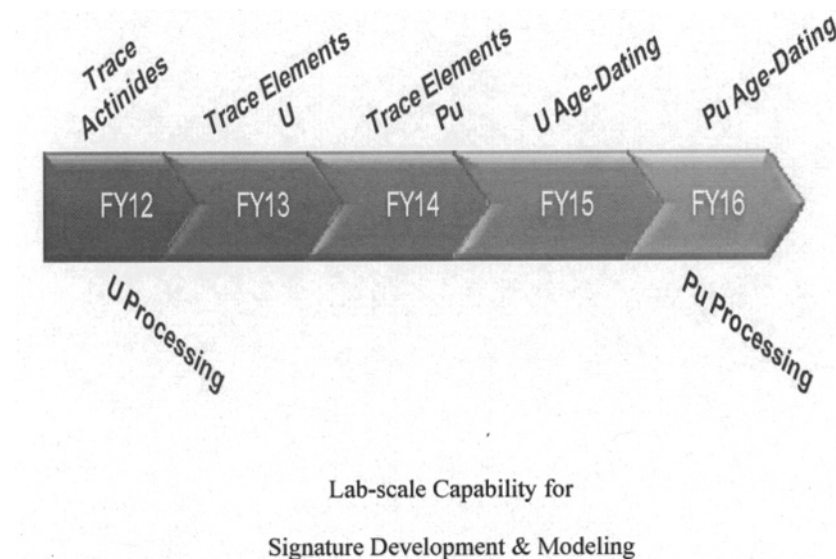
Objectives.—Our Focus:

- Advancing and validating lab analysis methods.
- Identifying discriminating signatures.
- Creating foundational standard reference materials.
- Developing tools to interpret and link lab measurements.
- Developing predictive models.

FISCAL YEAR 2012 PLANNED ACCOMPLISHMENTS/MILESTONES

- Develop standard reference materials that will aid in the validation of analytical methodologies, including the standard for trace actinides in bulk SNM.
- Continue development of benchmark analytical methodologies for determining trace actinides in bulk SNM.
- Continue to develop and validate predictive models and techniques to improve understanding of how lab-scale uranium processing capability for signature development and modeling purposes becomes operational.

GNDA Alignment.—GNDA performance goals—Aligns to national strategic 5-year plan for improving the nuclear forensics attribution capabilities of the United States (signed by the President April 30, 2010).

Methodology Benchmarking*RD&O—NTNFC PPA*

- Technology advancement, \$14,670,000.
- Operational readiness, \$4,360,000. (Not a systems development effort.)
- Expertise development, \$5,740,000. (Not a systems development effort.)

Technology Readiness Level.—All activities within the methodology development and signature development areas of Technology Advancement fall within TRL 3–7. Most of the activities fall within TRL 4–6, with transition to DOE or other inter-agency partners upon completion.

Timeline for Transition:

- One analytical method is scheduled for transition to operational use per year over the next 5 years.
- Uranium processing for signature development is scheduled for operational implementation in fiscal year 2012.
- Plutonium processing for signature development is scheduled for operational implementation in fiscal year 2016.

QUESTIONS SUBMITTED BY SENATOR FRANK R. LAUTENBERG

TRANSPORTATION SECURITY ADMINISTRATION

Question. There have been at least six security breaches at Newark Airport in the last 2 months. I understand that the Transportation Security Administration (TSA) is almost 70 employees short of its allocated number for Newark Airport. What is DHS doing to fully staff Newark Airport? Based on these incidents, what steps has TSA taken to improve training for transportation security officers and managers?

Answer. In close partnership with the Federal Security Director and staff at Newark Airport (EWR) the Transportation Security Administration (TSA) has initiated a robust and comprehensive effort to address EWR staffing vacancies, and EWR is currently scheduled to reach near-100 percent staffing by May 1. In the interim, TSA has been providing additional resources as needed. For example, TSA deployed additional Supervisory Training Instructors to train new—hires, additional AIT-certified Transportation Security officers (TSOs) to conduct daily operations while EWR TSOs are being trained, and additional staff resources to assist in Human Resources and Training operations.

Following a breach, a complete review of the incident is conducted and each action is broken down in detail to ascertain the reasons behind the breach. Every TSA individual involved in the activity and their response is included in this review. TSA employees identified as not having followed standard operating procedures or whose

actions are the result of inattention to duty are immediately removed from their position, and can only return to their positions if retraining and recertification for their positions is determined sufficient and is satisfactorily accomplished.

Question. The Transportation Security Administration (TSA) recently participated in a program at Newark Airport to help autistic children and their families prepare for air travel. The program included a flight simulation for the families as well as a well-attended voluntary training to increase autism awareness among Transportation Security officers (TSOs) and airline personnel. Currently, I understand that TSA provides 3 hours of disability-related training for new hires. Does TSA have any plans to improve coverage of autism and other types of neurodevelopmental disorders and cognitive disabilities in the new-hire and ongoing training for TSOs? What steps will be taken to improve the travel experience for passengers with autism and other types of neurodevelopmental disorders or cognitive disabilities?

Answer. The Transportation Security Administration (TSA) is in the process of updating all of its training with regard to persons with disabilities. In addition, TSA is working with Autism Explores and other similar programs to develop core training on autism for our screening personnel. This training focuses on the skills to screen those with disabilities with compassion, respect, and sensitivity while maintaining transportation security. TSA is also working with the Administration on Developmental Disabilities to ensure that information about TSA's screening procedures is accessible to people with cognitive disabilities.

MASS TRANSIT

Question. The Department's assessment of the Nation's passenger rail and mass transit systems—completed in October 2010—found that a significant security risk exists. Yet, surface transportation security continues to make up a very small percentage of the TSA's overall budget. Why doesn't the budget request for TSA reflect the risk to rail and transit?

Answer. In the aviation sector, the Federal Government has the primary role to provide security. This is accomplished primarily by funneling traffic at security checkpoints and by screening the passengers and baggage. In the surface modes, the primary responsibility of providing security rests with the local responders and the system operators, who are supported by TSA.

The President's fiscal year 2012 budget includes funding to enhance TSA's surface transportation efforts. The budget supports programs that are designed to assist the industry and State and local governments and transportation authorities to identify their vulnerabilities and provide guidance and tools to help close critical security gaps in high-risk systems. Specifically, the fiscal year 2012 request includes \$109 million to support 37 VIPR teams, including 15 teams dedicated to surface transportation security. The request also includes \$300 million for the Transit Security Grant Program to support State and local surface transportation efforts.

TRANSPORTATION SECURITY LABORATORY

Question. The Transportation Security Laboratory (TSL) in Atlantic City, New Jersey creates technology to mitigate impacts of potential terrorist attacks against our transportation system, but it is currently operating beyond its maximum designed capacity. While the budget requests \$18 million for facility renovations, the TSL needs additional funds to complete the renovations. Will you commit to providing all of the funds necessary to upgrade this facility and help TSA meet its safety mandates?

Answer. The Science and Technology Directorate (S&T) has a long-term plan for completing necessary upgrades to the Transportation Security Laboratory (TSL). S&T's 5-year plan for TSL upgrades began in fiscal year 2010 and will continue through fiscal year 2014, pending available appropriations. The high priority upgrades are targeted for completion first. The 5-year program will provide TSL with the critical infrastructure needed to ensure its role as a leader in transportation security, and to meet its mission of researching, developing, engineering, testing, and evaluating solutions to detect and mitigate the explosives threat and weapons used against our Nation's transportation systems.

PORT SECURITY GRANTS

Question. House Republicans have proposed cutting port security grants by two-thirds. The Port of New York/New Jersey is the largest port on the east coast and the second-largest port in the country. It is directly linked to what the FBI deemed the most dangerous area in America for a terrorist attack. Yet it would lose \$33 million in security funding under the House bill. What would be the impact on the

New Jersey-New York region and our Nation's economy if there were to be a terrorist attack on one of our largest ports?

Answer. Various studies indicate that the economic impact of a major terrorist attack on one of the Nation's largest ports could total in the tens of billions of dollars—though the impact would depend on the degree and severity of a terrorist attack. The goal of the Port Security Grant Program is to mitigate port security risks and address the gaps and vulnerabilities that may expose our ports to terrorist attack. Toward that end, the program has been highly successful; all large ports have made substantial progress toward addressing the risks identified in their port-wide risk management plans. Under significant budgetary constraints, DHS must prioritize funding allocation to those areas where it is most needed.

In 2007, our Nation's largest ports areas having the most risk developed port-wide risk management plans with PSGP dollars. These plans were developed to support the area maritime security plans and facility security plans. Through these plans, security vulnerabilities were identified and prioritized lists of projects to reduce these vulnerabilities were developed (spend plan). More than \$1 billion in PSGP funding has been allocated to planning and executing projects from these plans, with many more security risk mitigation projects yet to start and urgently dependent on future year funding. While the majority of PSGP funding goes to the largest port areas the program is equally vital to the smaller port areas and facilities to offset their associated security costs as well.

Below are examples of security activities and security risk mitigation projects that will be in jeopardy if funding is reduced:

- CBRNE response vehicles, the most common being small boats and the associated equipment, such as Forward Looking Infrared Radar (FLIR).
- Increasing the security of facilities by improving access control systems, monitoring and recording devices such as CCTV, fencing, bollards, and other perimeter security measures.
- Providing new capabilities for maritime law enforcement, including K-9 explosives detection teams, maritime security training, and patrol vessel tactical operations.
- Specialized maritime training and exercises such as dive training, suicide bomber, and active shooter training, and CBRNE response.
- Interoperable communications projects, including infrastructure upgrades, and mobile, portable, and base communications.
- Creating and enhancing interagency operations centers.

STATE AND LOCAL GRANTS

Question. The State and local grant programs put funding where it is most critical—on the front lines in the hands of first responders. I was pleased to see an increase in both of these programs in the President's request, but I was concerned that the House proposal for fiscal year 2011 would make cuts to both the Urban Area Security Initiative and the State Homeland Security Grant Program. What kinds of homeland security programs would receive less funding if those cuts were to take place?

Answer. There are two issues related to a potential reduction in funding for the Urban Areas Security Initiative (UASI) and the State Homeland Security Program (SHSP) grants. First, because there are statutory minimum allocations in the SHSP grants, funding for the highest-risk States could be reduced. Furthermore, any reduction in funding for these programs will result in the reduction or elimination of funding that historically goes toward planning, intelligence analysts, equipment (such as interoperable communications equipment), first responder training, and exercises.

QUESTIONS SUBMITTED BY SENATOR DANIEL COATS

AVIATION SECURITY FEES

Question. The budget proposes a new general appropriations bill provision to amend current law to allow aviation passenger security fees to be increased above the current statutory maximums. The fiscal year 2012 budget assumes the enactment of this provision and a fee increase of \$1.50 per enplanement beginning the third quarter of the fiscal year generating an additional \$589,940,000 in offsetting collections. Even if the requested authority was granted to you by the start of the new fiscal year, how realistic is it that a rulemaking could be executed and completed in time to enable an additional \$589,940,000 in fee collections to be generated in fiscal year 2012?

If the requested authority to allow you to increase the fee amount is not provided, what impact will this have on your fiscal year 2012 request? What specific reductions would you propose from the levels requested to make up for this nearly \$590 million budget shortfall?

Answer. The fiscal year 2012 budget request proposes the fee increase in the third quarter of fiscal year 2012 to provide sufficient time for the rulemaking process, assuming the Congress passes this proposal prior to end of fiscal year 2011.

Despite the Congress's original intent that the security fee covers nearly all costs related to passenger and property screening, the fee currently offsets less than one-third of the total cost of aviation security. At the same time, costs of security have continued to increase. In 2000, it cost less than \$1 to screen each passenger. In fiscal year 2010, the average cost for the Transportation Security Administration (TSA) to screen a passenger and baggage has increased to nearly \$9, in part to airline imposed checked baggage fees that have resulted in TSA screening 56 million additional carry-on bags at airport checkpoints annually.

I fully appreciate the constraints of the current fiscal environment, and it is precisely because of the current economic situation that I feel nothing should be left off the table to fund the Department's critical frontline operations. While airlines have increased fees across the board—from checked baggage and extra leg room to refreshments, we have never adjusted how we fund security measures to protect the traveling public.

I ask for your support of the administration's proposal to ensure that we are able to continue the significant progress we have made in enhancing aviation security while fulfilling the Congress's intent to do so in a fiscally responsible manner that does not penalize American taxpayers. I look forward to working with you on this matter in the coming months.

GRANTS EFFECTIVENESS

Question. What steps has the Department taken and planning to implement the recommendations made by the local, State, tribal, and Federal preparedness task force regarding developing measurements of the effectiveness of grants?

Answer. FEMA agrees with recommendation #14 in the Local, State, Tribal, and Federal Preparedness Task Force's report to the Congress, which calls for "Threat and Hazard Identification and Risk Assessment (THIRA) processes at all levels of government to establish a foundation to justify preparedness improvements." The detailed recommendation came directly from the stakeholder community.

FEMA has taken the recommendations from the local, State, tribal, and Federal preparedness task force report into consideration while working to improve coordination and consolidation of FEMA's grant programs, including coordinating inter-agency grant programs and more closely linking capability assessments to grant activities. FEMA has also contracted with the National Association of Public Administration (NAPA) to conduct a study to develop a core set of performance measures that can be used to track performance of the SHSP and UASI grants.

VISA WAIVER PROGRAM/BIOMETRIC AIR EXIT IMPLEMENTATION

Question. When does the administration plan to make a decision on implementing biometric air exit, or will it be officially proposing to repeal the biometric air exit requirement currently in statute?

Answer. Since the Congress enacted the statute that included a mandate for biometric air exit, DHS has implemented several automated systems based on biographic data that much more effectively capture arrival and exit information as compared to the processes in use at the time.

Additionally, DHS has conducted a number of pilots and studies since 2003 to assess options on how to meet the biometric exit mandate. The pilots have demonstrated that while the technology exists to collect biometrics—the costs associated with the operational facilities and staffing needs necessary to achieve effective compliance with biometric air exit requirements using currently available technology and processes are quite high, particularly when compared to any potential security gains. DHS does not invest money into solutions where the benefits are not commensurate with the costs incurred.

Accordingly, DHS will explore new biometric exit solutions that can be implemented in a cost-effective way, while simultaneously implementing enhancements to existing biographic exit systems. These enhancements will focus on strengthening Customs and Border Protection's (CBP) Advance Passenger Information System (APIS) information collection and carrier compliance auditing; enhancing US-VISIT's automated matching of arrival and departure records, review of records of potential overstays, and posting of "lookouts" for those who have overstayed.

Question. On December 8, 2010, President Obama met with Polish President Komorowski. During a press availability after the meeting, the Visa Waiver Program (VWP) came up. President Obama said: “I am well aware that this is a source of irritation between two great friends and allies, and we should resolve it. The challenge I have right now is, is that there is a congressional law that prevents my administration from taking unilateral executive action. So we’re going to have to work with the Congress to make some modifications potentially on the law. In the meantime, what I indicated to President Komorowski is that I am going to make this a priority. And I want to solve this issue before very long. My expectation is, is that this problem will be solved during my presidency.” How does the administration plan to fulfill the commitment President Obama made to the President of Poland in December 2010—to resolve the issues preventing Poland’s entry into the Visa Waiver Program—with the fiscal year 2012 budget proposal of no funding for biometric air exit?

Answer. As the President stated, the administration supports the inclusion of Poland in the Visa Waiver Program. However, as the President also indicated, the administration cannot take unilateral action on including Poland in the Visa Waiver Program due to the current rate of visa refusals from Poland pursuant to section 217 of the Immigration and Nationality Act. In addition, Poland has not yet met the other important requirements for designation in the Visa Waiver Program, such as concluding agreements to share criminal and terrorism screening data with the United States and entering into an agreement on reporting lost and stolen passports to Interpol.

RECAPITALIZATION OF THE U.S. CUSTOMS AND BORDER PROTECTION (CBP) AIR AND MARINE FLEET

Question. At the level of funding requested for fiscal year 2012 which funds two UH-60 helicopter conversions, CBP will still have to take as many as nine UH-60 helicopters out of service by 2014 due to age. What is the Department doing to mitigate this situation? Will other assets be redeployed?

Answer. CBP is continuing to pursue the aged aircraft engineering analyses, physical inspections, and service life risk assessments initiated in late fiscal year 2009 to determine how to keep the aircraft flying safely beyond current projections. Through this initiative, each aircraft is evaluated to determine if additional maintenance can extend the service life the aircraft beyond current projections. CBP is also considering an expansion of the mandatory 720-flight-hour inspection to include the inspection or replacement of selected high stress components and structural components to keep the aircraft in service longer. If an aircraft is not operational, it will be placed in controlled storage until it can be inducted into the Army conversion line, and the remaining assets will be reallocated to the agency’s highest-priority missions.

Question. What number of UH-60s would need to be converted from A to L in fiscal year 2012 and fiscal year 2013 to eliminate the need to take out of service nine UH-60 helicopters due to age in 2014?

Answer. CBP will continue its aged aircraft engineering analyses, physical inspections, and service life risk assessments to determine how to keep the aircraft flying safely beyond current projections. At CBPs request, the U.S. Army recently provided updated costs and possible induction schedules to mitigate the impact of the projected groundings. Based on the Army estimates, it is possible to induct up to three aircraft per year without a negative impact to the factory production schedule.

Question. What are the results of the investigations conducted by CBP into the age-related problems of the UH-60s? Are there revised estimates as to the cost of converting two UH-60s from A to L?

Answer. The Army has recently provided updated costs and possible induction schedules to mitigate the impact of the aged-aircraft situation. The costs are based on the age of CBP’s UH-60 Black Hawks and actual experience gained during the conversion of the first two aircraft over the past 2 years. The quantity of aircraft per year shows how CBPs assets might fit into the planned factory production schedule without an impact on the Army’s helicopter program. This accelerated schedule is expected to reduce the number of age-related groundings of CBP aircraft.

TACTICAL BORDER INFRASTRUCTURE

Question. In January of this year, the decision was made not to extend the Boeing contract for SBInet. Yet, the budget requests funds for three additional deployments of integrated towers with cameras and radars for fiscal year 2012. Are the contracts in place today to acquire these systems and deploy them?

Answer. The Integrated Fixed Tower (IFT) systems are not “additional deployments” of the SBInet Block 1 system that was procured under the Boeing contract. Following a departmentwide review of the SBInet program, I directed CBP to end SBInet as originally conceived and implement a new border security technology plan that will utilize existing, proven technology tailored to the distinct terrain and population density of each border region. Where appropriate, this technology plan will include elements of the former SBInet program that have proven successful, such as stationary radar and infrared and optical sensor towers. The Department does not intend to use the existing Boeing contract for procurement of any of the technology systems included in the new Southwest Border technology plan. In the future, the Department will conduct full and open competition of the elements in the new border security plan, including any expansion of the integrated fixed towers.

Question. If no contracts are in place now, is there a high level of risk that CBP will not be able to execute three deployments in fiscal year 2012?

Answer. There are certainly normal risks associated with awarding any contract, but we do not believe there is a high risk to being able to award the new Integrated Fixed Tower system contract during fiscal year 2012. Program planning is under way and CBP has already engaged industry and has conducted a significant amount of market research. There are multiple companies who have an integrated tower system already designed, developed, and in use today.

DHS HEADQUARTERS CONSOLIDATION

Question. What is the GSA cost associated with the Federal Emergency Management Agency (FEMA) building at St. Elizabeths? What is the DHS fiscal year 2012 cost being deferred? Show original project phases and funding estimates and how these will change with the deferral of the FEMA project. What is the impact of deferring the FEMA building? Provide the total current estimate of the St. Elizabeths DHS headquarters consolidation project. Is it still \$3.4 billion or has the estimate been revised?

Answer. The GSA costs for the FEMA building excluding parking and infrastructure on the East Campus is approximately \$215 million, which includes design and Management and Inspection (M&I).

The Department deferred \$108 million of the DHS costs associated directly with FEMA headquarters on the East Campus in order to fund frontline operations within the current budget environment.

The current St. Elizabeths development estimate is \$3.56 billion (\$1.37 billion for DHS and \$2.19 billion for GSA), subject to receipt of fiscal year 2011 appropriations as requested. This is a revision of the earlier development estimated costs and is based on the GSA prospectus submission for fiscal year 2011.

While the DHS estimate remains within the original programmatic estimate, GSA costs have increased from \$2.04 billion to \$2.19 billion due to the following:

- Stabilization of buildings as part of the site’s designation as a National Historic Landmark;
- Additional east campus infrastructure to disperse the density originally planned for the west campus as requested by consulting parties;
- Malcolm X/Interstate-295 highway interchange;
- Historic preservation measures per the programmatic agreement signed with consulting parties;
- New energy target mandates that were not required when the original cost estimates were made.

Significant delays caused by a lack of funding in fiscal year 2011 are expected to increase St. Elizabeths project costs. GSA and DHS continue to evaluate ongoing construction activities in light of resources provided in 2011 and will be able to provide new project cost estimates at a later date. Without full funding of the President’s fiscal year 2012 request, the cost and schedule impacts will be even greater.

DEVELOPMENT ESTIMATE AT THE INITIATION OF CONSTRUCTION FUNDING WITH FISCAL YEAR 2009 APPROPRIATIONS

[In thousands of dollars]

	Prior	Fiscal year 2009	ARRA	Fiscal year 2010	Fiscal year 2011	Fiscal year 2012	Fiscal year 2013	Fiscal year 2014	Fiscal year 2015	Fiscal year 2016	Total	Notes
GSA	64,447	346,639	447,773	277,875	312,875	288,375	298,375	2,036,359	(1)
DHS	100,278	248,116	347,575	209,734	277,860	203,839	9,754	19,405	1,416,561	(1,2)
Total	64,447	446,917	625,450	522,609	566,235	502,214	9,754	19,405	3,452,920	(1)
Phase 1	(6)
Phase 2A	(7)
Phase 2B	(8)
Phase 3	(9)

REVISED DEVELOPMENT ESTIMATE BASED UPON FISCAL YEAR 2011 PROSPECTUS AND FISCAL YEAR 2012 PRESIDENT'S BUDGET SUBMISSION

GSA	64,447	346,639	450,000	380,296	217,706	440,101	290,561	2,189,750	(1,3,5)
DHS	100,278	200,000	287,800	159,643	396,090	211,854	3,508	13,438	1,372,611	(1,3,4,5)
Total	64,447	446,917	650,000	668,096	377,349	836,191	502,415	3,508	13,438	3,562,361	(1)
Phase 1	(6)
Phase 2A	(7)
Phase 2B	(8)
Phase 3	(9)

- ¹ Indicates appropriations received prior fiscal year's through ARRA.
- ² Fiscal year 2009 DHS budget request was \$120 million. Received \$97,578 million in USCG and \$2.7 million in DHS appropriations.
- ³ Outyear estimates were adjusted based on receipt of ARRA funding.
- ⁴ DHS reduction from 2009 to current result of project team salaries and benefits moved to the CAO base.
- ⁵ Fiscal year 2012 President's request deferred FEMA by 1 year.
- ⁶ Indicates Phase 1 (USCG) completion schedule.
- ⁷ Indicates Phase 2A (DHS HQ and DHS operations centers (DOC)) facility completion schedule.
- ⁸ Indicates Phase 2B (FEMA) completion schedule.
- ⁹ Indicates Phase 3 (remaining components) completion schedule.

DOMESTIC NUCLEAR DETECTION OFFICE

Question. The fiscal year 2012 President's budget request again proposes to transfer the funding for Transformational Research and Development from the Domestic Nuclear Detection Office (DNDO) to the Science and Technology (S&T) Directorate. In addition, there have been a number of critical assessments of DNDO over the years, including its management of the Advanced Spectroscopic Portal program and the Cargo Advanced Automated Radiography System (CAARS). Given the difficulties that DNDO has had in the past with project management, what steps have been taken to improve project management at DNDO?

Answer. Over the last 2 years, DNDO has implemented a new process called the Solution Development Process (SDP) to implement Department of Homeland Security (DHS) Acquisition Directive (AD) 102-01. The SDP provides an effective strategy for program oversight by aligning strategic analysis, planning, and investment decisionmaking with a complementary process to design, develop, test, and deploy specific detection solutions. All of the projects within DNDO are being formally reviewed by DNDO senior management as part of the SDP process. The reviews are chaired by the DNDO Deputy Director, who also serves as the Component Acquisition Executive (CAE). These reviews address issues related to funding, staffing, scheduling, technical development, and risk. A formal SDP training program has been developed by DNDO so that all Program Managers fully understand the SDP and implement it correctly to ensure improved oversight and governance. The SDP, which is both calendar and milestone driven, comprises a series of development stages separated by formal stage gate decision reviews.

- Stage 0.*—Key strategic planning and gap identification.
- Stage 1a.*—DNDO-wide budgeting and needs prioritization.
- Stage 1b.*—Needs justification and capabilities development planning.
- Stage 2a.*—Alternatives analysis, piloting, operational requirements, and solution selection.
- Stage 2b.*—Detailed program planning and cost estimation.
- Stage 3.*—Detailed solution design, development, and testing.
- Stage 4.*—Production, deployment, and operation.

The first two stages (stage 0 and 1a) are conducted annually when the gaps in the Global Nuclear Detection Architecture (GNDA) are reviewed and needs are identified. The remaining stages are milestone driven and are not completed until all of the requirements of their respective stage gates are met. Detailed worksheets inform efforts at each stage to ensure that all aspects of the program are properly evaluated. The SDP accommodates materiel and nonmateriel solutions.

Additionally, DHS has implemented a departmentwide initiative to ensure that Program Managers are trained and certified at levels commensurate with the size, funding, and complexity of the programs they manage. This effort, intended to create a cadre of officially certified Program Management Professionals, is embraced by DNDO and enhanced through the SDP reviews. Achieving and maintaining the appropriate certification is included in the DNDO Program Managers performance goals. The combination of increased individual skill of those engaged in the acquisition process along with more rigorous procedures and oversight, as directed by DHS AD 102-01 and DNDO's SDP, help to ensure that DNDO's project management capabilities continue to improve.

Question. How will DNDO formalize the relationship with S&T to competently handle the movement of programs from Transformation Research and Development to Systems Development, which will remain with DNDO?

Answer. In order to maintain and improve the current levels of integration for transformational research and development activities and transitions of technologies for use by operators, DNDO will work closely with S&T to ensure that the pipeline for technological advancements remains coordinated to address gaps in the Global Nuclear Detection Architecture and operational needs by utilizing the integrated project team process to integrate research projects into future acquisition plans and develop formal technology transition agreements (TTAs). TTAs define the level of maturity of the technology at transition, ranging from commercially available to less mature stages, and solidify the expectations of the technology developer and the component who receives the technology. This arrangement will ensure a smooth integration of S&T developed technologies into the DNDO systems development process.

QUESTIONS SUBMITTED BY SENATOR THAD COCHRAN

DEPARTMENTAL MANAGEMENT

Question. Your Department has been operating under a continuing resolution for 5 months. Yesterday, Defense Department officials testified to our committee that operating in such a manner has “brutal” effects on the readiness of our Nation’s defense. Like the Defense Department, your Department’s ability to operate efficiently also has significant implications on our Nation’s security interests. What types of effects has operating under a continuing resolution for so long had on your Department?

Answer. The Department of Defense and Full-Year Continuing Appropriations Act enacted on April 15, 2011, provides resources to the Department for the rest of the fiscal year. DHS will be able to accomplish its mission within the funding levels provided in the continuing resolution.

Question. If the Congress is unable to enact some form of a Homeland Security appropriations bill for fiscal year 2011, what are some of the specific effects operating under a year-long continuing resolution would have on your Department’s missions?

Answer. The Department of Defense and Full-Year Continuing Appropriations Act enacted on April 15, 2011, provides resources to the Department for the rest of the fiscal year.

COAST GUARD

Question. The President’s fiscal year 2011 budget request included funding to complete the fifth national security cutter, yet there are funds requested in the fiscal year 2012 budget to finish out NSC #5. If there was a certainty that the Congress would appropriate these funds by October 1 of this year, this might be a reasonable plan. But understanding our current condition and recent history, would getting NSC #5 under contract before the end of fiscal year 2011 as previously planned create efficiencies and savings in the shipbuilding process?

Answer. Coast Guard is prepared to efficiently complete a contract for construction of NSC #5 as soon as full funding authority is enacted by the Congress.

NATIONAL SECURITY CUTTERS

Question. What does the timely acquisition of national security cutters mean to the Coast Guard’s fleet in terms of the retirement of other vessels, operations and maintenance costs, and personnel costs? How have the current national security cutters improved your capabilities?

Answer. The Coast Guard is committed to meeting its surface operational hours baseline to execute statutorily required missions in the deepwater environment. The Coast Guard is able to meet this baseline through the delivery of new assets to replace aging cutters. The sooner the Coast Guard can bring national security cutters (NSC), offshore patrol cutters (OPCs) and fast response cutters (FRCs) online, the sooner it can decommission its aging, legacy cutters. Furthermore, maintenance and repairs that are increasingly above programmed levels draw critical depot level maintenance funds from other assets, thereby impacting readiness across the fleet.

The following specific, unique and improved, operational features and capabilities allow NSCs to execute required missions:

- Long-range EEZ and border enforcement capability, with the endurance to remain on station for extended periods along with the speed and range to reach any area of operation.
- Long-range, high-speed counterterrorism, counter-drug intercept capability.
- Capabilities for continued operations in a contaminated environment (e.g., chemical, radiation).
- Three dimensional capable air-search radar, providing the capability to manage the air domain during regular or disaster operations.
- Three cutter boats. The stern ramp allows for extremely quick launching with only one or two persons on deck to conduct the launch. Fast action response teams are ready to respond to a tactical situation with very little advance notice.
- Two aircraft hangars allow the cutter to deploy with two aircraft, increasing aviation capabilities for prolonged aviation presence and increased redundancy for continued operations.
- Ability to exploit information on-scene, and exchange secure data to and from the national intelligence network. This capability is critical in conducting homeland security missions, including interdicting drug and human smuggling networks that benefit from increasing sophistication of IT systems.

As an example of the capabilities of the NSC, during her first patrol, utilizing advanced sensors, communications, and onboard cutter boats, the NSC *Bertholf* interdicted 12,500 kilograms of cocaine with a street value of nearly \$400 million and detained nine suspected drug smugglers in the Eastern Pacific.

ACQUISITION LONG LEAD TIME MATERIAL

Question. How would acquisition of long lead time materials for NSC #6 during fiscal year 2012 affect overall acquisition efficiency and contractor workload? Does the current plan to buy long lead time materials in fiscal year 2013 at the same time you buy the ship itself and conceivably sign a construction contract reduce or raise the overall price of the ship as opposed to buying long lead time materials in advance?

Answer. The funding associated with the sixth NSC is not required until fiscal year 2013.

DISASTER RELIEF

Question. Over the past 20 years, more than \$4 out of every \$5 appropriated by the Congress to the Disaster Relief Fund (DRF) have been provided through supplemental appropriations bills. Over the past 20 years, an average of nearly \$7 billion annually has been appropriated for disaster relief, yet you requested only \$1.95 billion for fiscal year 2011 and \$1.8 billion for fiscal year 2012. Your budget documents state that these requested funds are only for “noncatastrophic disaster activity.”

Many experts I’ve talked to say that true catastrophes only occur once every 20–25 years. What is your definition of catastrophe? Does it match the definition of catastrophe as provided in the Post-Katrina Emergency Management Reform Act? How often do catastrophes occur in your mind? Are we budgeting wisely for disasters?

Answer. A total of 22 events that qualify as catastrophes have occurred in 14 of the last 23 fiscal years. While no hard definition currently exists, FEMA currently believes that an event qualifies as a catastrophe if the estimated cost-threshold to the Federal Government is more than \$500 million.

The \$1.8 billion requested for the DRF, per standard annual practice, reflects the 5-year rolling average of historical obligations for noncatastrophic events (those less than \$500 million in estimated obligations), less estimated recoveries for fiscal year 2012. This methodology is one that the administration has proposed in its fiscal year 2010 and fiscal year 2011 budgets and represents the best use of available information in developing the DRF request. We also have a robust strategy in place to deobligate funds from past contracts and projects that are now complete and where we did not spend all the money originally obligated. Based on our experience in actively managing the unliquidated contract obligations in fiscal year 2010, we are taking the same approach for individual assistance and public assistance grants in fiscal year 2011, and anticipate that our projected recoveries may be higher than previously estimated. Regardless, we are committed to working with the Congress to ensure that the DRF remains solvent through fiscal year 2011 and fiscal year 2012.

U.S. CITIZENSHIP AND IMMIGRATION SERVICE DATA CENTER CONSOLIDATION

Question. Your Department has received recognition for its data center consolidation efforts. These efforts are particularly impressive when considering the number of previously unaffiliated agencies your Department has brought together.

What types of efficiencies will your Department gain from these efforts? Can you quantify current or future taxpayer savings as a result of these efforts?

Answer. The following are types of efficiencies that the Department of Homeland Security (DHS) expects to gain from the data center consolidation efforts:

- Provide operational efficiencies and economies of scale through the consolidation of more than 30 locations to 2;
- Facilitate management, sharing and dissemination of data;
- Provide improved disaster recovery and Continuity of Operations (COOP) capabilities;
- Enhance Department’s ability to quickly launch new departmentwide capabilities;
- Provide components single storefront for ordering of services;
- Improve server (CPU) utilization (percent); rack space utilization (percent); rack floor utilization (percent); power usage/square foot; and power usage effectiveness;

—Standardize IT resource acquisitions across Components, as well as streamline maintenance and support contracts that will allow for less complex vendor support to expedite response times in the event of an emergency.

To date, five legacy data centers have completed their migrations to the DHS Enterprise Data Centers of a total of 43 identified primary sites for a combined short term savings of \$16.3 million/year. The long term return on investment (ROI) analysis, which factors in legacy data center costs, costs to migrate to the two DHS data centers, and projected operations and maintenance (O&M) costs, anticipates cumulative savings/cost avoidance from our Break Even Point in fiscal year 2017 through fiscal year 2030 of \$4.8 billion.

COAST GUARD UNMANNED AERIAL VEHICLES

Question. With the successes of unmanned systems in the wars in Iraq and Afghanistan, why doesn't your fiscal year 2012 budget request contain funding to move the Coast Guard closer to using unmanned aerial vehicles in its operations?

Answer. The Coast Guard continues to work with the U.S. Navy and Customs and Border Protection to advance application of these capabilities in the maritime domain. As these technologies and capabilities are further researched and developed for maritime applications, the Coast Guard is focusing capital resources toward high priorities within the Coast Guard Air Domain, including extending service life and enhancing the capability of current airframes such as the H-65, H-60, and C-130H as well as recapitalizing aged air assets (e.g. replacing the HU-25 Falcon with the HC-144A Ocean Sentry).

Question. As the Coast Guard continues to analyze options for land-based unmanned aerial vehicles, has it considered any fee-for-service maritime surveillance UAV options as demonstrated in SOUTHCOM's Project Cazador that could mitigate immediate risk to the Coast Guard with regard to acquisition, training, basing, and the like?

Answer. Yes, the Coast Guard had representatives from the Research and Development and Requirement and Capabilities staffs on site during the 2010 Project Cazador and considers fee-for-service to be one of several means to conduct a land-based Unmanned Aircraft System (UAS) technology demonstration. The Coast Guard continues to work with Department of Homeland Security (DHS) partners to leverage their experience and investments in land-based UAS technology.

TSA'S ADVANCED IMAGING TECHNOLOGY

Question. Following the Christmas Day bombing attempt of 2009, your Department moved quickly to aggressively procure Advanced Imaging Technology in an attempt to keep up with current air travel threats. Could you update the subcommittee on the progress of that effort and whether these machines are providing both enhanced detection capability and sufficient passenger privacy?

Answer. Advanced Imaging Technology (AIT) units detect a wide range of metallic and nonmetallic threats, including explosives, on passengers. By the end of fiscal year 2012, assuming full funding of the Department's fiscal year 2011 and fiscal year 2012 budget requests, TSA estimates that 1,275 AITs will be deployed.

Rigorous privacy safeguards are also in place to protect the traveling public. All images generated by imaging technology are viewed in a walled-off location not visible to the public. The officer assisting the passenger never sees the image, and the officer viewing the image never interacts with the passenger. The imaging technology that TSA uses cannot store, export, print, or transmit images. Furthermore, to further enhance privacy protections in place for AIT screening, TSA is currently testing Automated Target Recognition technology, which generates a generic outline of a person and identifies the approximate area on the figure where an anomaly is detected.

FEMA'S MAP MODERNIZATION

Question. As you know, much of my State of Mississippi and Senator Landrieu's State of Louisiana is protected from flood waters by levees. Having intimately experienced Hurricane Katrina, we take seriously the need of the National Flood Insurance Program to accurately reflect risk to the public. However, Senators from all over the Nation are hearing from their constituents regarding FEMA's Map Modernization efforts. Do you share my view there are practical changes we can make to FEMA policy that might mitigate some of the concerns of communities without adversely affecting risk identification or the solvency of the NFIP?

Answer. Since fiscal year 2009, we have been implementing the Risk Mapping, Assessment, and Planning (Risk MAP) program, which not only addresses gaps in flood hazard data, but uses that updated data to form a solid foundation for risk

assessment and floodplain management, and to provide State, local, and tribal entities with information needed to mitigate flood related risks. Risk MAP is introducing new products and services extending beyond the traditional digital flood maps produced in Flood Map Modernization, including visual illustration of flood risk, analysis of the probability of flooding, economic consequences of flooding, and greater public engagement tools. FEMA is increasing its work with officials to help use flood risk data and tools to effectively communicate risk to citizens, and enable communities to enhance their mitigation plans.

Currently, FEMA is executing the National Flood Insurance Program (NFIP) Reform work plan, and is considering proposed legislative, regulatory, and administrative changes to the program. This process was designed to engage program stakeholders from a variety of perspectives, and to date has included hundreds of stakeholders in a series of public meetings and generated thousands of public comments on reform possibilities.

The original NFIP reform work plan envisioned an 18-month process, to ensure thorough and transparent engagement with a wide variety of program stakeholders. Based on feedback from the Congress, FEMA has accelerated this schedule by 6 months, and expects to report findings by the end of the fiscal year. This will allow for consideration of program reforms by decisionmakers prior to the expiration of the current NFIP authorization in September 2011.

QUESTION SUBMITTED BY SENATOR LISA MURKOWSKI

U.S. COAST GUARD MARITIME COVERAGE IN ALASKA

Question. In Alaska, we are very concerned with the President's decision to decommission another high endurance cutter in the fiscal year 2012 budget. Given the vast maritime environment that the Coast Guard is responsible for protecting in Alaska, I am concerned that the decommissioning of these cutters will have significantly negative impacts on the safety and security of the Alaskan commercial fishing industry. The Coast Guard is tasked with conducting operations in Alaska that encompasses more than 3,800,000 square miles, which is larger than the land mass of the continental United States, and more than 33,000 miles of coastline. With the Alaskan fishing industry producing more than 60 percent of the national fishing totals each year, the cumulative loss of another cutter potentially from the west coast could place a significant portion of the Alaskan fishing fleet that routinely operate in the Bering Sea and gulf of Alaska in danger as well as preventing the Coast Guard from effectively ensuring that the safety and commercial fisheries regulations are adequately enforced.

Previously you testified that your Department and the Coast Guard were committed to a plan to recapitalize the current high endurance cutter fleet with new national security cutters, an effort that was designed to maintain current cutter coverage levels while quickly brining the new class of cutters online. However, the fiscal year 2012 proposed budget does not have any funding for the long lead time items for the sixth national security cutter. Yet your Department supports the President's proposed budget to decommission another high endurance cutter before a suitable replacement comes online. By delaying the purchase of the long lead time items, it appears to me that your Department and the administration are not fully committed to the Coast Guard's recapitalization efforts. It seems unfeasible for the Coast Guard to be able to protect the maritime public of Alaska with the continued pace of their cutter decommissionings. What plan do you have in place to assure that there is adequate cutter coverage in Alaska?

Answer. The Coast Guard has and will continue to serve in Alaska with the existing fleet of high endurance cutters (WHEC) and new national security cutters (NSC). The USCGC *Bertholf* has been certified ready for operations and is conducting its first 110-day patrol in Alaska this spring. USCGC *Waesche* will be ready for operations by November 2011. USCGC *Stratton* will be delivered in September 2011 and ready for operations in the spring of 2013. These NSCs will be homeported on the west coast and will provide greater operational availability than the aging WHEC hulls they are replacing. The Coast Guard will leverage these and other assets to meet Bering Sea presence requirements in order to execute critical living marine resources, other law enforcement, and search and rescue missions.

SUBCOMMITTEE RECESS

Senator LANDRIEU. Unless there are further comments or questions, which I do not think there will be, this meeting is recessed.

[Whereupon, at 11:50 a.m., Wednesday, March 2, the subcommittee was recessed, to reconvene subject to the call of the Chair.]